Military Health System (MHS) Information Assurance (IA) Policy/Guidance Manual

February 12, 2003

Version 1.3

Prepared By:
Military Health System (MHS)
Information Assurance (IA) Program Office

EXECUTIVE SUMMARY

In October 1997, the Assistant Secretary of Defense for Health Affairs and the Service Surgeons General authorized development of a plan for the consolidation of the Military Health System (MHS) Information Technology (IT) program development, management functions, and personnel to improve efficiency and effectiveness. Their vision included the creation of a professional, accountable, and customer-driven organization that effectively and consistently provides secure, high-quality information.

This *MHS Information Assurance (IA) Policy/Guidance Manual*, as presented by the MHS Chief Information Officer (CIO), provides the requisite policy and guidance needed to ensure that sufficient security safeguards are implemented within the MHS to comply with the DoD's Defense-in-Depth IA strategy. This policy/guidance is policy for all MHS centrally managed Automated Information Systems (AISs) and networks under the authority of the MHS CIO. Additionally, this document is policy for the AISs and networks developed and operated by the TRICARE Management Activity (TMA).

Notwithstanding any other interpretation of views, nothing in this document shall be construed to obligate the Services and/or their subordinate organizations to achieve any level of compliance, performance, adherence, or oversight related to this document. Furthermore, it is explicitly and un-equivocally noted herein that adoption, adherence, compliance and implementation, or performance with any of the prescriptive requirements herein are at the sole option and discretion of the Service's and subordinate organizations in the performance of their missions and in the employ of applications and technology covered within the scope of this document while on their respective installation(s) without regard to which organization or program manager ultimately funded, designed, developed, fielded, or sustains the technology or application. To maximize standardization of security across the MHS, the Service Medical Departments are encouraged to use this document as IA guidance for the AISs and networks developed, managed, and operated by the Services. Given the aforementioned clarification of scope and applicability, it is explicitly noted that service and service medical department policy and procedure shall take and retain precedence over the guidance contained herein. To that end, Service organization specific (e.g., base/post/station or intermediate commands) questions pertaining to applicability, interpretation, compliance, and implementation of this policy should be directed through your chain of command to your service specific medical information activity.

This Manual has been developed to document the roles, responsibilities, and policies required to secure AIS and networks within the MHS. IA is based on five security concepts: availability, integrity, authentication, confidentiality, and non-repudiation. These concepts are interwoven throughout the Manual and provide the framework for the development of technologies and policy. Technical and administrative IA policy and guidance for the MHS is presented along with an overview of security certification and accreditation. Due to the emerging enhanced requirements to protect patient identifiable data, this Manual also addresses the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.

It is understood that the policy and guidance provided is subject to revision based on the dynamic nature of information security technologies, DoD and Federal policy, and public law.

Table Of Contents

Table of Figures

Appendices

1.0 INTRODUCTION

The Military Health System (MHS) increasingly depends upon Information Technology (IT) to accomplish its mission. IT offers the potential for providing more efficient and effective health care management over paper-based procedures. However, with the advances in technology and the interconnectivity of Automated Information Systems (AIS), MHS AIS and networks are at risk of attack by numerous elements, both internal and external to the MHS. Recognizing the importance of protecting patient information, the MHS Chief Information Officer (CIO) established the Information Assurance (IA) Program Office. The Information Assurance Program Office has established a proactive approach to information systems security. This proactive approach integrates the development of sound policy, guidance, best practices, training, and management controls necessary to achieve information assurance.

Policy and guidance address roles and responsibilities, as well as the development, use, configuration, management, security design, and training issues associated with the successful production, deployment, and management of secure AISs and networks. Upper management's early and continuous involvement is critical to the success of any organization's IA program. Responsibility for management and the development of controls in these areas are clearly established and assigned throughout the MHS enterprise and fully supported by operational and technical controls.

The implementation of these controls also allows the MHS to achieve compliance with the multi-layered Defense-in-Depth IA (DiD) strategy that has been directed by DoDD 8500.1, "Information Assurance (IA)." Figure 1 illustrates the components of DoD's Defense-in-Depth Strategy for IA.

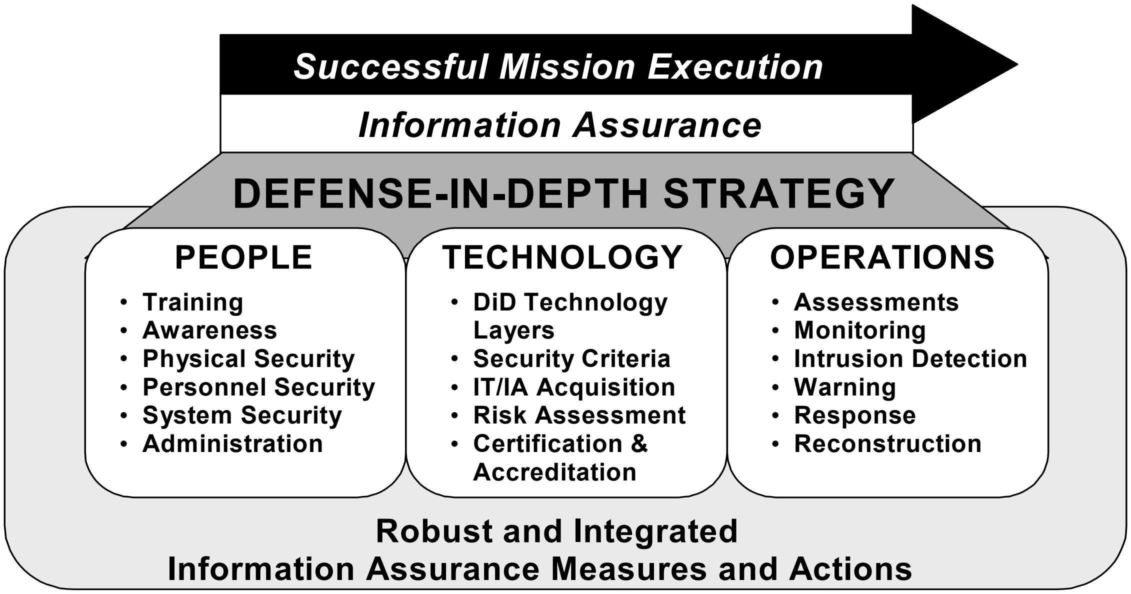


Figure 1. Defense-in-Depth Strategy

The MHS Information Assurance Program Policy Manual was originally developed by the Information Assurance Program Office in 1996 to provide policy and guidance for the secure operation of MHS AISs. Because of the rapid advancements in technology, the dramatic increase in attacks on systems, and additional security requirements mandated by the DoD, this Manual has been developed to address these changes and the additional security requirements.

Adherence to the provisions in this Manual ensures that an appropriate and consistent level of security is achieved to maintain availability, integrity, authentication, confidentiality, and non-repudiation of MHS' Sensitive But Unclassified (SBU) AISs and networks. The protection of MHS' mission-critical/mission essential AISs and networks and SBU information is an absolute priority to provide world-class health support to the warfighter and beneficiaries during peacetime and wartime. Medical information has been determined to be sensitive but unclassified (SBU) and is to be handled in accordance with the Policy/Guidance Manual. Classified medical data will not be gathered, stored, transmitted, or processed on unclassified systems.

1.1 PURPOSE

This Manual provides policy and guidance for incorporating security safeguards directed by the DoD. Also provided is information on security best practices developed as a result of a partnership of DoD, National Institute of Standards and Technology (NIST), National Security Agency, corporate America, and other organizations committed to sharing lessons learned in efforts to achieve IA on a global scale.

1.2 SCOPE

The provisions of this Manual apply to all military, civilians, and contractors who manage, design, develop, operate, or access Tri-Service (centrally managed) AISs and networks, and AISs and networks developed and operated by the TRICARE Management Activity (TMA). Government Owned, Contractor Operated (GOCO) and Contractor Owned, Contractor Operated (COCO) AISs that process DoD SBU information are also subject to the provisions of this Manual and DoD IA policies.

This policy/guidance is policy for all MHS centrally managed AISs and networks under the authority of the MHS CIO. Additionally, this document is policy for the AISs and networks developed and operated by TMA.

Notwithstanding any other interpretation or views, nothing in this document shall be construed to obligate the Services and/or their subordinate organizations to achieve any level of compliance, performance, adherence, or oversight related to this document. Furthermore, it is explicitly and un-equivocally noted herein that adoption, adherence, compliance and implementation or performance with any of the prescriptive requirements herein are at the sole option and discretion of the Service's and subordinate organizations in the performance of their missions and in the employ of applications and technology covered within the scope of this document while on their respective installation(s) without regard to which organization or program manager ultimately funded, designed, developed, fielded, or sustains the technology or application. To maximize standardization of security across the MHS, the Service Medical Departments are encouraged to use this document as IA guidance for the AISs and Networks developed, managed, and operated by the Services. Given the aforementioned clarification of scope and applicability, it is explicitly noted that service and service medical department policy and procedure shall take and retain precedence over the guidance contained herein. To that end, Service organization specific (e.g., base/post/station or intermediate commands) questions pertaining to applicability, interpretation, compliance, and implementation of this policy should be directed through your chain of command to your service specific medical information activity.

1.3 IMPLEMENTATION PLANNING

The MHS Information Assurance Office is currently developing the MHS Integrated IA Implementation Plan, which will provide IA implementation guidance. Upon finalization and publication of the Implementation Plan, this Manual will be updated with appropriate references.

1.4 MHS INFORMATION ASSURANCE (MHS IA) POLICY STATEMENT

It is MHS policy that:

a. SBU information be continuously protected from unauthorized access, use, modification, or disclosure.

b. SBU information be protected at all times and in all forms (i.e., raw input data, data stored in AISs, and output products).

c. SBU information be processed, stored, transmitted, and produced only on accredited AISs and networks.

d. AIS and network managers ensure that AISs and network security is an integral part of the life-cycle management (LCM) of AISs and networks.

e. Appropriate physical, administrative, and technical safeguards be implemented, enforced, and maintained to provide the most cost-effective security safeguards for each AIS and network.

f. Implemented safeguards are consistent with the approved MHS architecture to ensure integration and interoperability.

g. Procedures are developed and implemented to control access to Tri-Service and TMA AISs and networks.

h. Until the appropriate security investigation paperwork has been completed and submitted, and initial IA security awareness training has been completed, personnel employed to fill Automated Data Processing (ADP)/Information Technology (IT) I, II, or III positions will not be granted access to Tri-Service or TMA AISs and networks or Contractor AISs that process patient information.

i. Personnel employed to fill ADP/IT I positions will not be granted access to Tri-Service or TMA AISs and networks or contractor AISs that process patient information until the background investigation (BI) is completed and they have completed the initial IA security awareness training.

j. All MHS centrally managed systems shall be assigned a mission assurance category (MAC) by the system owner. The MAC is directly associated with the importance of the information the systems contain relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Requirements for availability and integrity are associated with the mission assurance category, while requirements for confidentiality are associated with the information classification or sensitivity and need-to-know. Both sets of requirements are primarily expressed in the form of IA controls and shall be satisfied by employing the tenets of defense-in-depth for layering IA solutions within a given IT asset and among assets; and ensuring appropriate robustness of the solution, as determined by the relative strength of the mechanism and the confidence that it is implemented and will perform as intended. The IA solutions that provide availability, integrity, and confidentiality also provide authentication and non-repudiation.

1.5 PROGRAM OBJECTIVES

The MHS IA Program Office has identified the following IA objectives:

a. **Availability** – Assure information and communications services will be ready for use when expected.

b. **Integrity** – Assure information will not be accidentally or maliciously altered or destroyed.

c. **Authentication** – Assure that the identity of a user, device, or other entity in a computer system is positively identified as a prerequisite to allowing access to resources in an AIS or network.

d. **Confidentiality** – Assure that information is not disclosed to unauthorized persons, processes, or devices.

e. **Non-repudiation** – Assure that the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

Best practices show these objectives will be met by establishing an IA Program Office; implementing Federal and DoD IA policies; and performing C&A activities in accordance with DoD Instruction (DoDI) 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)." Development of this MHS IA Policy/Guidance Manual, performing periodic inspections, training, assigning responsibility, and holding personnel accountable will further help meet the above objectives.

1.6 MHS IA POLICY/GUIDANCE MANUAL UPDATES

This IA Policy/Guidance Manual is the primary means for issuing IA policy. The Manual will be updated as necessary when the Services, DoD, or higher authority promulgates either new policy or an update to published policy or change is required for any other reason, such as correction, omission, or clarification. The entire Manual will be reviewed for currency whenever a change is issued, so that the Manual is current as of the change date. New policy and updates will be researched, developed, and presented for review and approval following the process in Section 1.6.1 (*Policy or Policy Change Development)*. When approved, new policy and policy changes will be issued as changes to the IA Policy/Guidance Manual. These updates will become effective and are to be implemented on the date that they are signed. After five (5) published changes, the Manual will be reprinted incorporating all changes.

1.6.1 Policy or Policy Change Development

It is the responsibility of the Service representatives to the IAWG to review new Service policy or updates to published Service policy and assess their impact on policy or guidance in this IA Policy/Guidance Manual. Service representatives to the IAWG will develop changes for the modification, inclusion, or exclusion of specific sections of this IA Policy/Guidance Manual. Changes identified by any of the Services will be prepared by the MHS IA Program Office and presented to the IAWG for information, comment, and proposed alternative resolutions within 60 days of submission. These changes will also be distributed to the Services for concurrence. Upon concurrence, the proposed changes will be adopted at the next IAWG meeting.

New DoD or higher authority IA policy or changes to existing IA policy will be reviewed by the IA Program Office to assess their impact on policy or guidance in this IA Policy/Guidance Manual.

The following process affords IA representatives from the Army, Navy, and Air Force Surgeons General offices, Program Executive Office, TMA directors, and the Technical Integration Working Group (TIWG) an opportunity to influence proposed policy. The process is described in **Figure 2**, New Policy and Policy Update/Revision Process Flowchart.

a. When new policy or a change to existing policy is required, the IAWG's Service representatives or the TMI&S IA office will develop a draft of the policy or change to this IA Policy/Guidance Manual.

b. IAWG members are presented with proposed IA policy or policy changes for review, comment, and coordination.

c. After IAWG coordination, the draft policy will be presented to the TIWG for their information and comment.

d. The draft policy will then be briefed to the MHS CIO to request his approval to present the draft policy to the Information Management Program Review Board (IM PRB) for its approval.

e. When approved by IM PRB, the draft policy is returned to the MHS CIO for signature.

f. The signed policy will be promulgated for implementation to MHS PEO offices and TMA directorates, and as guidance to the Service medical departments.

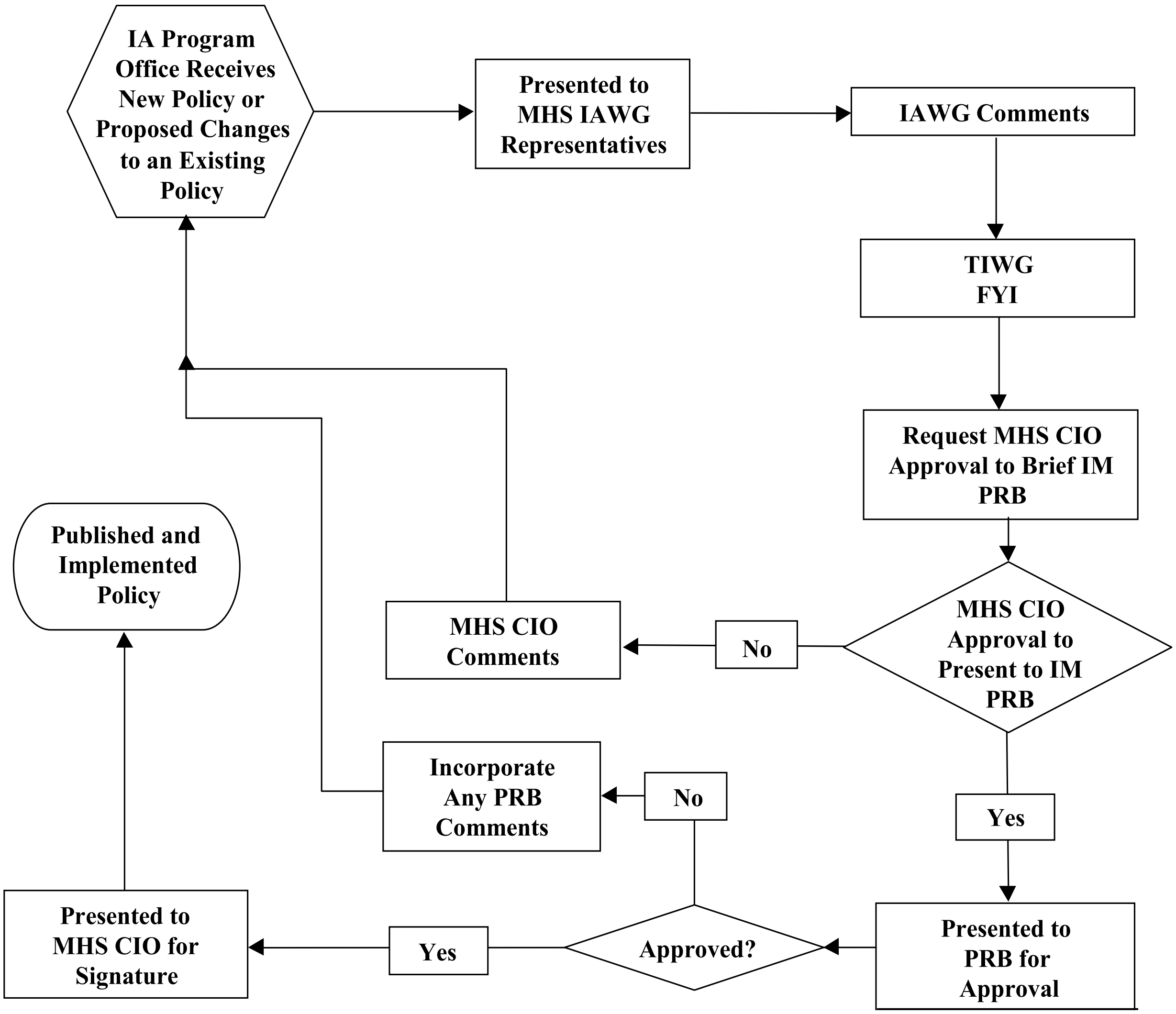

IA Program Office Receives New Policy or Proposed Changes to an Existing Policy
Presented to MHS IAWG Representatives
IAWG Comments
TIWG FYI
Request MHS CIO Approval to Brief IM PRB
MHS CIO Approval to Present to IM PRB
No
MHS CIO Comments
Yes
Presented to PRB for Approval
Approved?
No
Incorporate Any PRB Comments
Yes
Presented to MHS CIO for Signature
Published and Implemented Policy

Figure 2. New Policy and Policy Update/Revision Process Flowchart

2.0 ROLES AND RESPONSIBILITIES

2.1 Overview

One of the most important elements of the MHS IA Program is ensuring that all personnel are aware of their roles and corresponding responsibilities in maintaining the security of Tri-Service and TMA AISs, networks, and SBU information. Personnel who manage, design, develop, program, operate, or use Tri-Service or TMA AISs and networks have responsibilities that contribute toward the success of the MHS IA Program. This section describes the IA roles and responsibilities of the MHS CIO, Designated Approving Authority (DAA), Designated Approving Authority Representative (DAAR), MHS Program Executive Officer (PEO), Program Managers (PMs), IA personnel, and users.

2.2 The MHS Chief Information Officer (CIO)

The MHS CIO is responsible for the IA Program within the MHS. CIO responsibilities include:

a. Ensuring that IA is integrated into all policies and procedures used to plan, procure, develop, implement, and manage the MHS infrastructure and systems, as well as TMA developed systems.

b. Ensuring that IA is integrated into the MHS enterprise architecture.

c. Ensuring that MHS architectures are consistent with current and planned computing and communications assets within the Global Information Grid (GIG).

d. Appointing a qualified person to fill the position of Chief, Information Assurance Program Manager.

2.3 Designated Approving Authority (DAA)

MHS DAAs are appointed by the Assistant Secretary of Defense (Health Affairs) (ASD(HA)). A DAA shall be appointed for each DoD information system operating within or on behalf of the Department of Defense, to include outsourced business processes supported by private sector information systems and outsourced information technologies. The DAA shall be a U.S. citizen, a DoD employee, and have a level of authority commensurate with accepting, in writing, the risk of operating DoD information systems under his or her purview.

DAAs are responsible for:

a. Reviewing and approving AIS and network security safeguards, and issuing accreditation statements for each AIS and network under the DAA's jurisdiction based upon the acceptability of the security safeguards for the AIS.

b. Granting an Interim Approval to Operate (IATO) for an AIS or network to process information based on preliminary results of a security evaluation of the system. The

IATO covers the period of time determined in the certification process to resolve security issues required to meet Approval to Operate (ATO) accreditation.

c. Ensuring AISs under development are accredited prior to deployment or fielding.

d. Identifying security deficiencies and, where the deficiencies are serious enough to preclude accreditation, taking action to achieve an acceptable security level.

e. Verifying that data ownership, accountability, access rights, and special handling requirements are established for each AIS/network under his/her jurisdiction.

f. Verifying that an appropriate mission category has been assigned for each AIS/network under his/her jurisdiction.

g. Ensuring that Information Systems Security Managers (ISSMs), Information Systems Security Officers (ISSOs), and System Administrators (SAs) are designated for all systems under his/her jurisdiction, and that they receive the level of training necessary and appropriate certification to perform the tasks associated with his/her assigned responsibilities.

h. Ensuring that a process for reporting security incidents and lessons learned is established.

i. Ensuring that security safeguards approved during accreditation are implemented and maintained throughout the system life-cycle.

j. Ensuring that a security awareness and training program is implemented for all Tri-Service and TMA AIS and network users, to include developers, operators, and managers.

k. Documenting Memorandums of Agreement (MOAs) to address security requirements between AISs that interface or are networked, and are managed by different DAAs.

l. Documenting MOAs to address security requirements between AISs that interface or are networked to non-DoD entities.

m. Ensuring the reaccreditation of AISs and networks at least every three years, or whenever previously accredited systems undergo major modifications.

n. Appointing Designated Approving Authority Representatives (DAARs)/Certifiers.

2.4 CHIEF, INFORMATION ASSURANCE PROGRAM MANAGER

Responsibilities of the Chief Information Assurance Program Manager include:

a. Establishing, managing, and assessing the effectiveness of the MHS IA Program.

b. Development of Security Policy.

c. Ensuring Risk and Vulnerability Assessments are accomplished for all Tri-Service AISs and networks. (Service specific systems/networks are the responsibility of the Service Medical CIOs.)

d. Providing C&A services.

e. Providing security architecture support.

f. Ensuring security awareness training is conducted.

g. Managing the IAVA program.

h. Providing security product evaluation and testing.

2.5 DESIGNATED APPROVING AUTHORITY REPRESENTATIVE (DAAR)

DAARs are appointed by the DAA. The role of the DAAR is to implement the overall security requirements of the AISs under his/her area of responsibility. It is the responsibility of the DAAR to ensure that AIS modules, components, and applications are designed, developed, installed, and maintained by organizations where the AIS resides.

General duties of the DAAR include:

a. Ensuring reaccreditation of each AIS takes place at least every three years, or when major modifications are made to previously accredited systems.

b. Ensuring that security safeguards approved during accreditation are implemented and maintained throughout the system life-cycle.

c. Ensuring data ownership is established for each AIS to include accountability, access rights, and special handling requirements.

d. Approving alternative safeguards (i.e., physical or administrative) to attain the requisite AIS security level when implementing computer-based safeguards would be inefficient, or would impair operational effectiveness to an unacceptable degree.

e. Taking action to achieve an acceptable security level when AIS security deficiencies preclude accreditation.

f. Ensuring security officials are named for each AIS and are properly trained.

g. Ensuring a security education and training program is implemented for all AIS users, developers, operators, and managers using on-line, hard copy, or instructor-lead training.

h. Ensuring program implementation of MHS Computer Event Reporting and Tracking advisories.

i. Implementing MOAs to address security requirements between AISs that interface or are networked, and are managed by different DAAs.

j. Implementing MOAs to address security requirements between AISs that interface or are networked to non-DoD entities.

k. Approving an initial Interim Approval to Operate (IATO). Subsequent IATO requests must go to the DAA.

2.6 CERTIFICATION AUTHORITY (CA)/CERTIFIER

With the release of the DoD 8510.1 Manual, "Department of Defense Information Technology Security Certification, and Accreditation Process Application Manual," July 2000, the Certification Authority (CA) title has been shortened to Certifier. Therefore, it should be noted when CA is referenced in this Manual, CA and Certifier are the same person. The CA is designated by the DAA with the authority to establish and manage the organization's C&A program and to verify and validate AIS and network security design and implementation through testing and review of system security documentation. General duties of the CA include:

a. Ensuring that risk analysis and security evaluations are completed prior to AIS and network certification.

b. Certifying the extent to which AISs and networks meet prescribed security requirements.

c. Preparing the AIS and network C&A report and, upon the completion of certification, forwarding the report with any recommendations on accreditation to the DAA. Maintaining and providing other records and reports of C&A activities, as necessary.

2.7 MHS PROGRAM EXECUTIVE OFFICER (PEO) FOR INFORMATION TECHNOLOGY (IT)

Deputy Secretary of Defense Memorandum, "Defense Acquisition," October 30,2002, identifies the PEO as a military or civilian official who has primary responsibility for directing several major defense acquisition programs and for assigned major system and non-major system acquisition programs.

Within MHS, the MHS PEO for IT is responsible for the supervision and senior management of all Tri-Service PMs. As such, the MHS PEO for IT provides guidance, direction, and oversight to Tri-Service PMs. The MHS PEO for IT and subordinate PMs are responsible for ensuring that all IA requirements are met for AIS and networks under his/her authority.

2.8 PROGRAM/PROJECT MANAGERS (PMS)

PMs are responsible for the security posture of an AIS, network, or application and its data. General duties include:

a. Working closely with the Chief, Information Assurance Program Manager in administering the MHS IA Program.

b. Ensuring resources are budgeted and available (funding & personnel) to implement and maintain required Certification and Accreditation (C&A) security safeguards.

c. Ensuring the development and implementation of a C&A Plan for each AIS and network under his/her authority.

d. Ensuring the participation of AIS and network security personnel early in the development life-cycle to assist in the identification and selection of appropriate security controls, and to provide guidance on the accreditation process.

e. Writing one or more MOAs as necessary to address security requirements between: AISs that interface, AISs that are networked and are managed by different DAAs, or AISs networked to non-DoD entities.

f. Verifying the correct design of AIS and network security for systems under his/her authority.

g. Verifying the correct implementation of security design in the developed AIS and network by ensuring thorough security testing has been performed.

h. Initiating protective or corrective measures if a security problem arises.

i. Acting to achieve acceptable security levels when AIS and network security deficiencies preclude accreditation.

j. Ensuring that security controls are maintained throughout the system's life-cycle.

k. Ensuring that functional managers have properly identified and classified all information in the system or application.

l. Ensuring that quality assurance reviews are performed to minimize the risk of errors and ensure the integrity of the system and data.

m. Monitoring the contractors under his/her authority with access to Tri-Service and TMA AISs and networks, to ensure compliance with approved policies, procedures, and standards.

n. Providing assistance as needed to security personnel during the accreditation and reaccreditation processes.

o. Ensuring compliance with the MHS Information Assurance Vulnerability Alert (IAVA) Program.

2.9 INFORMATION ASSURANCE (IA) PERSONNEL

2.9.1 Information Systems Security Manager (ISSM)

Responsibilities of the ISSM include:

a. Serving as the focal point for policy and guidance on IA matters within his/her activity or system.

b. Providing policy and program guidance to subordinate activities.

c. Establishing, managing, and assessing the effectiveness of, and having overall responsibility for, the IA Program within his/her activity.

d. Ensuring compliance with approved MHS IA policies and procedures.

2.9.2 Information Systems Security Officer (ISSO)

ISSOs ensure that the systems under their purview are operated and maintained at the appropriate level of security. They oversee the implementation of system security requirements and monitor AIS and network security operations. The ISSO is the overall system security expert and coordinates IA issues with the MHS PEO for IT and staff with regard to IA. The ISSO also serves as an advisor to the CA, the ISSM, and the DAA. ISSO duties include:

a. Ensuring that AISs and networks are operated, used, maintained, and disposed of in accordance with security policies and practices.

b. Enforcing IA policies and safeguards on all personnel having access to the AIS and network for which the ISSO has cognizance.

c. Complying with DoD 5200.2-R, “Personnel Security Program,” concerning personnel security clearances and the designation of ADP/IT positions and security investigation requirements.

d. Ensuring that users have the required authorization and Need-to-Know, have been indoctrinated, and are familiar with internal security practices before granting access to the AIS or network.

e. Preparing a C&A Plan for AISs and networks, which provides responsibility and timelines for risk analysis, data collection, security evaluation, and report generation.

f. Ensuring AIS and network security safeguards appropriate to the system are addressed in system documentation.

g. Ensuring the periodic review of audit trails.

h. Reporting security incidents in accordance with procedures outlined in Section 5.11.

i. Reporting on the IA posture of the information system as required by the DAA.

j. Maintaining an AIS and network security plan, in accordance with DoD policies.

k. Ensuring consistent progress toward accreditation of all production systems under their auspices.

l. Ensuring IAVA procedures are followed in accordance with Appendix E.

m. Ensuring the development, maintenance, and periodic testing of Continuity of Operations Plan (COOP) and Disaster Recovery Plan (DRP).

2.9.3 System Administrator (SA)

Responsibilities of the SA include:

a. Ensuring servers, workstations, peripherals, communication devices, and application software are available to support users.

b. Ensuring anti-virus software is installed, maintained, and updated on all servers and workstations under his/her purview.

c. Assisting the ISSO in maintaining system configuration controls and Need-to-Know information protection mechanisms.

d. Advising the ISSO of security anomalies or integrity deficiencies.

e. Administering user identification or authentication mechanisms of the system.

f. Performing system backups, software upgrades, and system recovery, including the secure storage and distribution of backups and upgrades.

g. Working closely with the ISSO, SAs enforce password control, set permissions, perform security management functions, and coordinate system preventative and corrective maintenance problems with the Network Security Officer (NSO).

h. Thoroughly understanding the customer’s mission, be completely knowledgeable of the MHS capabilities and limitations, and the MHS IA Policy/Guidance Manual requirements.

i. Coordinating Help Desk support as required.

2.9.4 Network Security Officer (NSO)

NSOs ensure that security procedures and protocols governing AIS and network operations are developed, issued, and maintained for AISs and networks under their purview. General duties of the NSO include:

a. Serving as the point of contact for AIS and network security issues.

b. Issuing AIS and network security requirements, reviewing AIS and network configuration changes, working closely with ISSOs, and coordinating the submission of AIS and network C&A documentation through the ISSM.

c. Preparing, disseminating, and maintaining plans, instructions, and guidance concerning the security of the AIS and network.

d. Documenting and reporting any identified vulnerabilities to the ISSO.

e. Immediately reporting to the ISSO system failures that could lead to unauthorized disclosure or any attempt to gain unauthorized access to MHS sensitive information.

f. The NSO/ISSO is responsible for the configuration and monitoring of the Intrusion Detection System (IDS). Tri-Service Infrastructure Management Program Office (TIMPO) provides the MHS with the tools, knowledge, advice, and assistance to establish and maintain IDSs.

2.9.5 Help Desk Technicians (HDTs)

HDTs are the focal point for users reporting workstation or network access problems, and for obtaining technical assistance. General duties of HDTs include:

a. Troubleshooting user workstation problems and determining the proper course of action to rectify the problem.

b. Maintaining a historical database of problems with associated resolutions.

c. Implementing and maintaining the account and password management program.

d. Monitoring AISs and networks for attempts to subvert security controls.

e. Reporting security incidents to the NSO and the ISSO.

2.10 END USERS

Users are responsible for:

a. Observing regulations and guidance governing the secure operation (e.g., protection of passwords) and authorized use of AISs.

b. Immediately reporting all security incidents, potential threats, and suspected vulnerabilities to the appropriate ISSO or ISSM.

c. Completing initial and annual security awareness training.

3.0 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

The MHS has a longstanding commitment to protecting patient identifiable data (PID) and SBU information. The foundation for this commitment, while focusing on defense readiness, is based in significant part on the Privacy Act of 1974. This section provides an overview of additional requirements as mandated by HIPAA and its implementation.

3.1 OVERVIEW

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, (Public Law 104-191), requires that national standards be created and met to better ensure the safety and integrity of health care information existing in electronic form. Under HIPAA, entities electronically maintaining or transmitting health information will be required to incorporate reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of information. The following are the five (5) standards of the legislation:

- Transactions and Code Sets
- National Provider Identifier
- National Employer Identifier
- Security
- Privacy

3.2 HIPAA SECURITY STANDARDS

The security standards portion of HIPAA (currently in draft) aims to protect systems and their associated data from unauthorized access and misuse. Adopting appropriate security measures to proactively combat any anticipated threats or hazards to the security or integrity of information, as well as preventing unauthorized use or disclosure of information, will be expected of system users and administrators. Final HIPAA security standards, to include encryption of health care information, are currently under final review. Upon finalization of the specific security requirements, an MHS HIPAA Security Process will be developed and this Manual will be updated to reflect those requirements.

When the HIPAA security rules are finalized, it is anticipated that the MHS will develop and implement plans to ensure full compliance for Tri-Service AISs by the dates mandated by law.

4.0 CERTIFICATION AND ACCREDITATION (C&A)

4.1 OVERVIEW

Security C&A within the DoD is accomplished in accordance with the DoDI 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)." It implements the policies defined in DoDD 8500.1, "Information Assurance (IA)," Public Law 100-235 (1987), Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," and DoDD 5220.22, "Industrial Security Program." The DITSCAP applies to all components of the DoD, their contractors, and agents. Additionally, it is used by milestone decision authorities when acquiring IT, and for the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified, SBU, or classified information.

The DITSCAP implements policy, assigns responsibilities, and prescribes procedures for C&A of IT, AISs, and networks. A key benefit in the development of the DITSCAP is the creation of the C&A Process, which formalizes what needs to be accomplished to achieve C&A of unclassified, SBU, and classified IT/AIS and networks. DITSCAP is the standard DoD process for identifying information security requirements, providing security solutions, and managing IT/AIS and network security activities. The primary purpose of the process is to protect and secure the elements that make up the Defense Information Infrastructure, regardless of owner, Service, or Agency. DoD published the DITSCAP Application Manual, DoD 8510.1-M, July 31, 2000, in order to standardize the C&A process throughout the Department. Through the DITSCAP, the risk of introducing a non-secure system into a secure, shared environment is minimized.

> **Note:** *The C&A and Automated Data Processing (ADP) background investigation requirements apply to contractors that manage, design, develop, operate, or access MHS systems/networks and data. Government Owned Contractor Operated (GOCO) and Contractor Owned Contractor Operated (COCO) systems/networks that process MHS SBU information are also bound by these requirements. The only exception is when the contractor owned and operated information technology system has no connectivity with a DoD AIS or network. Then, DITSCAP C&A requirements do not apply. Additionally, background investigations for contractor personnel are not required and other safeguards may be used, such as, non-disclosure agreements and documentation training.*

4.2 MHS CERTIFICATION AND ACCREDITATION (C&A) POLICY

It is MHS policy that all AISs and networks be certified and accredited or re-accredited in accordance with DoDI 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)." Accreditation will be maintained during the AIS/network life-cycle phases of acquisition, operation, and sustainment. The MHS IA Program Office is responsible for ensuring the C&A process is compliant with the DITSCAP and for tracking of accreditations. DAAs, the MHS PEO for IT, and PMs are responsible for the accreditation and reaccreditation of AISs and networks under their purview. For AISs and networks under development, PMs, PEO, and the MHS IA Program Office share the responsibility for ensuring

C&A is accomplished prior to the AIS and network being deployed, fielded, or becoming operational. Contractor systems/networks that process MHS SBU information are also subject to the C&A process in accordance with the note in paragraph 4.1 above. The MHS IA Program Office stands ready to assist and provide guidance to accomplish C&A of Tri-Service AISs and networks. AIS and network security personnel will maintain updated copies of the following publications:

a. DoDI 5200.40, "Defense Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997.

b. DoD 8510.1-M, "Department of Defense Information Technology Security Certification and Accreditation Process Application Manual," July 31, 2000.

c. DoDD 8500.1, "Information Assurance (IA)," October 24, 2002.

4.3 DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

The following information is provided to the reader as an introduction to the DITSCAP. The four phases of the DITSCAP, security requirements, and risk assessment are introduced. Managers responsible for ensuring their systems are certified and accredited in accordance with the DITSCAP policy are encouraged to ensure their personnel receive appropriate training in the DITSCAP process.

4.3.1 The System Security Authorization Agreement (SSAA)

The SSAA is the key to DITSCAP. The SSAA is a formal agreement among the DAA(s), CA, the IT/AIS and network user representative, and the Program Manager. The SSAA establishes the level of security required before the system development begins, or when changes to a system are made. The SSAA is used to guide and document the C&A and the implementation of AIS and network security requirements. It is used throughout the entire C&A process to guide actions, document decisions, and specify IT/AIS and network security requirements. The SSAA resolves the following issues:

a. The schedule for the planning and certification actions.

b. Budget – The SSAA identifies all costs relevant to the C&A process. The Program Manager adds a C&A funding line item to the program budget to ensure the funds are available. Funding covers all costs associated with the certification, test development, and testing, and accreditation.

c. Functionality of the system – The operational and security functionality of the system.

d. Minimizes documentation requirements by consolidating applicable information into the SSAA (security policy, concept of operations [CONOPS], plans, architecture description, etc.).

4.3.2 DITSCAP Phases

The DITSCAP is implemented in four phases: Definition, Verification, Validation, and Post Accreditation.

4.3.2.1 Phase 1-Definition

This phase focuses on understanding the Information System (IS) business case or mission, environment, and architecture to determine the security requirements and level of effort to achieve accreditation. The objective is to agree on the system mission, operating environment, security requirements, C&A boundary, schedule, level of effort, and resources required. This phase incorporates the creation of the SSAA.

4.3.2.2 Phase 2-Verification

This phase corroborates the system's compliance with the information security requirements and constraints specified in the SSAA. The objective is to certify that the IS or components meet the security requirements.

4.3.2.3 Phase 3-Validation

This phase confirms compliance by an independent validation of the fully integrated system with the security policy and operational requirements of the SSAA. The objective is to produce evidence to support the DAA in making an informed decision to grant approval to operate the system (accreditation or IATO).

4.3.2.4 Phase 4-Post Accreditation

The Post Accreditation phase includes activities to monitor system management and operation to ensure an acceptable level of residual risk is preserved. Security management, change management, and annual compliance validation reviews are conducted.

4.3.3 Security Requirements

Security requirements are derived from policy, which states the minimum safeguards needed to protect AISs and networks, and the information they process. Those safeguards consist of, but are not limited to, administrative, personnel, physical, environmental, and technical controls which shield the AIS and network against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, modification, destruction, and data disclosure. Requirements should be satisfied through a combination of automated and manual means in a cost-effective and integrated fashion. It is important to stress that all MHS and contractor AISs and networks must be evaluated under the minimum security standards which are discussed in Paragraph 4.3.3.1.

AISs and networks must meet mandated Federal and DoD security requirements and specific mission security requirements. Security requirements are developed from the following publications:

a. DoDD 8500.1, “Information Assurance (IA).”

b. DoD 5400.11-R, “Department of Defense Privacy Program.”

4.3.3.1 The Trusted Computer System Evaluation Criteria

Policy for the trusted computer system evaluation criteria is provided in DoDD 8500.1, “Information Assurance (IA).” Its purpose is to provide technical hardware/firmware/software criteria and associated technical evaluation methodologies in support of the overall AIS and network system security policy, evaluation and approval/accreditation responsibilities. Use of DoDD 8500.1, “Information Assurance,” is mandatory for all DoD Components and their contractors for carrying out AIS and network system technical security evaluation activities applicable to the processing and storage of SBU, DoD information. A trusted computing base (TCB) is defined as: Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy.

Figure 3 below illustrates the security requirements followed by definitions for each requirement.

SECURITY REQUIREMENTS
• Discretionary Access Control • Object Reuse • Identification • Authentication • Audit • System Architecture • System Integrity • Security Testing • Security Features User’s Guide (SFUG) • Trusted Facility Manual • Test Documentation • Design Documentation

Figure 3. Security Requirements

a. **Discretionary Access Control** – This means to restrict access to objects based on the identity and need-to-know of users and/or groups to which the object belongs. Controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (directly or indirectly) to any other subject.

b. **Object Reuse** – Reassignment and re-use of a storage medium containing one or more objects after ensuring no residual data remains on the storage medium.

c. **Identification** – Process an IS uses to recognize an entity.

d. **Authentication** – Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

e. **Audit** – Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

f. **System Architecture** – Create and maintain a domain for execution to protect the Trusted Computing Base (TCB) from external interference or tampering, so the TCB may protect its resources via access controls and audit trails.

g. **System Integrity** – Attribute of an IS when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

h. **Security Testing** – Process to determine that an IS protects data and maintains functionality as intended.

i. **Security Features User's Guide (SFUG)** – Guide or manual explaining how the security mechanisms in a specific system work.

j. **Trusted Facility Manual** – Document containing the operational requirements; security environment; hardware and software configurations and interfaces; and all security procedures, measures, and contingency plans.

k. **Test Documentation** – Document describing the test activities and the results of the security mechanisms' functional testing.

4.4 REACCREDITATION

4.4.1 Three-year Cycle

In accordance with the DITSCAP, AISs and networks shall be reaccredited every three years, or sooner if a significant change to hardware, software, or environment occurs.

4.4.2 AIS and Network Modification

The following is a list of events affecting security that may require AIS and networks to be re-certified and reaccredited:

a. Hardware additions, changes, or upgrades requiring a change in the approved security countermeasures.

b. Software (operating system or applications) additions, changes, or upgrades providing security features.

c. Mission changes requiring a different security mode of operation.

d. Breaches of security or system integrity, or unusual situations that appear to invalidate the accreditation by revealing flaws in security design.

e. Significant changes in the physical structure of the facility.

f. Significant changes in operating procedures.

g. System configuration changes (e.g., a workstation connected outside of the approved accreditation parameters).

h. Inclusion of additional (separately accredited) system(s) affecting the security of that network.

i. Modification/replacement of a subscribing system affecting the security of that network.

j. Results of an audit or external analysis.

4.5 SECURITY LIFE-CYCLE PHASES

This section provides an overview of the life-cycle phases of an AIS/network and a summary of the security activities that take place during each of the life-cycle phases. The life-cycle processes shall be performed to produce qualitative results that provide management with prioritized security risks upon which to base decisions for system upgrades, certification, and accreditation.

4.5.1 Life-Cycle Management (LCM)

The functional process improvement required by OMB Circular A-130, “Management of Federal Information Resources,” needs to occur prior to initiation of the Security LCM phases. This involves the identification of unmet functional requirements that cannot be addressed adequately by existing systems, Commercial-off-the-Shelf (COTS) products, or by existing capabilities in other organizations inside or outside of the government. These unmet functional requirements become the justification for developing new systems or modifying existing systems to satisfy deficiencies in mission capabilities. The Security LCM process is an integral part of any system creation or modification effort.

AIS and network Security LCM incorporates operational requirements for security in all AIS and network planning and design, as well as ensuring that there is conformance with applicable security regulations, policies, and requirements. The product of this activity is the Mission Needs Statement (MNS) and the Operational Requirements Document (ORD). The organization sponsoring the system development initiative shall have an understanding of the nature of, and need for, information processed by the system and for a determination of the information’s sensitivity and criticality. Information sensitivity and criticality are determined by considering the need for data confidentiality, availability, and integrity during all phases of the life-cycle. Information developed from this activity is incorporated into the MNS and the Management Plan (MP) for the AIS.

Security activities implemented during a typical system life-cycle occur at various intervals in accordance with the phases of the AIS and network security life-cycle process. The phases, as described in DoD 8510.1-M, “DITSCAP Application Manual,” are shown in **Figure 4**. In addition, all systems requiring major AIS and network review need to comply with the requirements of DEPSECDEF Memorandum, “Defense Acquisition,” October 30,2002. These activities, existing within each life-cycle phase, may apply to enhancements to existing systems, COTS products/components, and new systems.

DISA has developed “NIPRNet Ports & Protocols Security Technical Guidance,” February 2002 (Draft). When signed, the MHS systems under development must comply with the intent of the document as part of the overall security preparations built into each MHS system and network.

SECURITY LIFE-CYCLE PHASES
▪ Concept Exploration and Definition. ▪ Demonstration and Validation. ▪ Development. ▪ Production and Deployment. ▪ Operations and Support.

Figure 4. Security Life-Cycle Phases

5.0 ADMINISTRATIVE INFORMATION ASSURANCE (IA)

Security measures in support of IA rely on both technical and non-technical countermeasures. This section addresses numerous administrative IA topics including: personnel security, security awareness, password control, marking and labeling, contingency planning, security assessments, risk management, and Federal ethics for use of the Internet and e-mail. Additional measures may be imposed by PMs, ISSOs, and other managers to protect sites and systems, as long as the measures are consistent with and in accordance with policy and guidance.

5.1 PERSONNEL SECURITY PROGRAM

The MHS Personnel Security Program is a set of procedures for implementing DoD policy and guidance that pertains to granting access to AISs, networks, and SBU information. A level of trustworthiness will be established before granting personnel access to MHS, and contractor AISs and networks or SBU information. The MHS IA Program Office, in compliance with DoD 5200.2-R, "Personnel Security Program," requires all military, civilian, and contractors who manage, design, develop, operate or access a Tri-Service AIS or network, or process DoD information to undergo an appropriate background investigation and security awareness training before access is granted to an AIS or network or DoD information. The type of investigation will depend on the ADP/IT position the employee is hired to fill.

The Office of the Assistant Secretary of Defense (OASD) verifies the clearances of military personnel prior to assignment to a position with the TMA. Federal civilian personnel also have background investigations performed on them as part of the hiring process.

5.1.1 Automated Information System (AIS) and Network Access Policy

It is MHS policy that:

a. Access to MHS AISs or networks will not be granted, except as noted below, until the appropriate background investigation is completed with favorable results and initial user security training is accomplished.

b. Interim access to the HA/TMA Network may be granted by the Director, Network Operations. Interim access to Service Networks/AISs is granted in accordance with Service protocol.

c. The Personnel Security Program within the MHS will be conducted in accordance with DoD 5200.2-R, "Personnel Security Program."

d. Contractors will ensure that when contract personnel leave a program (or terminate employment) the TMA/IMT&R Director, Network Operations Office is notified immediately, to accommodate the prompt removal of the individual(s) name(s) from the personnel security database.

e. Per guidance from the Office of Personnel Management (OPM), temporary employees and summer hires (under 120-day appointment) are not normally processed for a suitability investigation; however, Commanders may require the individual to complete a Standard Form (SF) 85-P to conduct a local suitability review prior to granting access to unclassified information or systems. Individuals will be briefed on accountability requirements prior to being granted access.

f. The number of persons cleared for access to AISs and networks be kept to a minimum, consistent with the requirements of operations.

g. Each user will receive initial and annual security and awareness training focusing on his/her responsibilities for the use, protection, and release of information as described in this Manual. Paragraph 5.7 of this Manual, *Security Training and Awareness Program*, contains the specifics.

h. The local ISSO or local Service-designated representative is responsible for initial and annual security and awareness training.

i. Program offices will send monthly updated lists from the personnel security access database to the TMA/IMT&R Director, Network Operations Office showing required additions, deletions, etc. It is noted that the Services will use Service specific protocols for updating their personnel security access database.

j. Federal civilians will be investigated as part of their hiring process.

k. Contractors must submit evidence of prior investigations or current security clearance if applicable for review to ensure that the investigation was conducted at an acceptable level. If a previous investigation was not conducted, contractors must apply to the OPM/Defense Security Service (DSS) to initiate investigations and obtain clearances for the ADP/IT positions to which they have been assigned.

l. Temporary system/maintenance personnel will not have unescorted access to AIS/networks.

5.1.2 Automated Data Processing (ADP)/Information Technology (IT) Positions and Required Investigations

The following chart, **Figure 5**, shows the investigation requirement for each level of ADP/IT position.

Level	Investigation Requirement
ADP/IT-I	Background Investigation (BI)
ADP/IT-II	DoD National Agency Check Plus Written Inquiries (DNACI) or National Agency Check Plus Written Inquiries (NACI)
ADP/IT-III	National Agency Check (NAC) or Entrance National Agency Check (ENTNAC).

Figure 5. ADP/IT Position Investigation Requirements

5.1.3 Personnel With Current Security Clearances

Typically, individuals who possess an active security clearance for information based upon an investigative scope that meets or exceeds that necessary for assignment to an ADP/IT position do not require further investigation. The clearance provides the basis for issuance of a trustworthiness determination without further investigation or adjudication unless:

a. Significant derogatory information that was not previously adjudicated becomes known or

b. There has been a break of 24 months or more in the individual's military service, DoD civilian employment, or access to classified information.

5.1.4 Administrative Investigations

The DSS conducts personnel security investigations for access to classified information and ADP/IT I and III levels for military, DoD civilian, and contractor personnel. The OPM conducts personnel security investigations for ADP/IT II levels.

5.1.4.1 Federal Civilian and Military Personnel Investigations

The Washington Headquarters Services (WHS) is responsible for ensuring all government personnel are processed for security clearances or ADP/IT access, as TMA duties require, before they are assigned to TMA. The WHS personnel security program is accomplished in accordance with DoD 5200.2-R, "Personnel Security Program." The TMA Director of Network Operations receives the results of ADP/IT investigations, retains a copy, and forwards the original to the requesting official. Results of security clearances are received by the TMA Office of Administration, who notifies the appropriate TMA office.

5.1.4.2 Contractor Investigations

Contractors will:

a. Submit ADP/IT personnel security investigation request to the Contracting Officer's Technical Representative (COTR) Program Manager and/or Lead Agent for approval.

b. Complete electronic version of ADP/IT personnel security investigation questionnaire.

c. Forward completed ADP/IT personnel security investigation questionnaire to OPM/DSS, as required.

d. Provide the TMA Program Manager and/or Lead Agent with a list of personnel submitted for security investigation processing by OPM/DSS.

5.1.5 Separation of Duties

Separation of duties is the practice of dividing the steps in a critical function among different individuals. For example, one system programmer can create a critical piece of operating system code, while another authorizes its implementation. OMB Circular A-123, "Management

Accountability and Control," requires that key duties and responsibilities in authorizing, processing, recording, and reviewing official agency transactions should be separated among individuals, and that managers should exercise appropriate oversight to ensure that individuals do not exceed or abuse their assigned authorities.

Such a control keeps a single individual from subverting a critical process. It makes the compromise of a system difficult without collusion. This provides checks and balances to enhance the integrity of the AIS, the network, and the information. Specific emphasis should be made on separation of duties between security and operations functions of an organization. Security personnel must have both the authority and system access to provide oversight of security-related functions in any AIS and network.

OMB Circular A-130, "Management of Federal Information Resources," requires the incorporation of personnel security controls, such as separation of duties.

It is MHS policy that:

To avoid a conflict of interest, separate persons will hold the two positions in each item below:

a. System Developer -- System Tester

b. Programmer -- Code Reviewer

c. System Administrator -- Information Systems Security Officer (ISSO)

d. System Administrator -- Security Auditor

e. Data Entry Person -- Reviewer of audit trails and transaction logs

5.2 PASSWORD CONTROL

5.2.1 User Password Responsibilities

User identification and password systems support the minimum requirements of accountability, access control, least privilege, and data integrity. These mechanisms are often the most cost-effective and efficient method of achieving the minimum-security requirements. The security that is provided by such a system depends upon the password being kept confidential at all times. Other techniques, such as biometrics access control devices or smart cards provide practical alternatives for use in conjunction with, or in place of, password systems.

It is MHS policy that:

a. Users will change their password the very first time they log on to an AIS or network.

b. Passwords will be eight (8) alphanumeric characters in length (at minimum) and consist of a mix of upper and lower case letters, numbers, and special characters.

c. Words found in a dictionary are not to be used as passwords.

d. Users will not write down their password.

e. Users will protect their password from disclosure.

f. Users are responsible for memorizing their password.

g. User passwords will not be shared.

h. User passwords will be changed every 90 days.

i. Users will notify the ISSO or designated representative immediately of password disclosure, misuse of the system, or other potentially dangerous practices.

Note: Training is the key for safeguarding passwords. Users must be trained in the proper use, creation, issuance, and storage of passwords and in the policies pertaining to them. See Paragraph 5.7, *Security Training and Awareness Program*, of this Manual for additional information.

5.2.2 System Administrators (SAs) and Information Systems Security Officers (ISSOs) Password Responsibilities

Computer Security Center Standard 002-85, “DoD Password Management Guideline” (Green Book), was developed to assist in providing credibility of user identity by presenting a set of good practices related to the design, implementation, and use of password-based user authentication mechanisms.

It is MHS policy that:

a. The features and practices described in CSC-STD-002-85, “Department of Defense Password Management Guideline, 12 April 85,” be incorporated into Tri-Service and TMA AISs and networks.

b. SAs and ISSOs be familiar with and enforce the guidelines for issuing and safeguarding identifications (IDs) and passwords.

c. A password be initially assigned to a user when enrolled on the AIS or network.

d. The AIS will be configured to force users to change their initial password the first time they logon to the system.

e. The AIS will be configured to force users to change their password every 90 days.

f. The AIS maintains a password database.

g. Passwords be eight (8) alphanumeric characters in length (at minimum) and consist of a mix of upper and lower case letters, numbers, and special characters.

h. Words found in a dictionary shall not be used as passwords.

i. Single characters not be repeated more than twice in a password.

j. The number of password attempts will be limited to three (3) attempts before the user is locked out of the system.

k. The user will be notified at least five days prior to password expiration.

l. The reuse of the current password and five prior passwords is prohibited when changing the current password.

5.2.3 First Line Supervisors Password Responsibilities

First line supervisors are normally the first to know when a subordinate no longer requires access to the AIS or network. The prompt revocation of access to an AIS or network when access is no longer required, for what ever reason, must be accomplished.

It is MHS policy that first line supervisors will immediately notify the ISSO/SA when an employee's access to the AIS or network is no longer required.

5.3 Disposition of Unclassified Hard Drives

Disposition of unclassified DoD hard drives will be accomplished in accordance with the Assistant Secretary of Defense (ASD) Memorandum, "Disposition of Unclassified DoD Hard Drives," June 4, 2001. The ASD's memorandum and included attachments provide policy for the proper sanitation and disposition of unclassified hard drives. Specifically, it addresses disposition of hard drives in three cases: DoD-owned computers, leased computers, and warranty repair or replacement (DoD-owned or leased computers).

The ISSO will ensure disposition of DoD hard drives is accomplished in accordance with this policy.

5.4 Copyrighted Software

Software purchased by the government is driven by the terms and agreements established by the vendor through the procurement process. Copyright and licensing agreements must be honored and the software must be tracked to ensure compliance. Managers who purchase software that is protected by quantity licenses must ensure that a system is in place to control copying and distribution.

It is MHS policy that:

a. Only government purchased software will be installed on Tri-Service AISs and networks.

b. Activities with a mission-related requirement for installing other than government purchased software must obtain a waiver from the ISSO.

c. Users abide by Section 106 of Title 17, United States (U.S.) Code, *Copyrights*, which gives copyright owners exclusive rights to reproduce and distribute their material.

d. Copyrighted software products not be reproduced except to the limit provided by contract (e.g., archive copy for backup).

5.5 Automated Information Systems (AISs)/Networks Physical Security

Physical security is the action taken to protect information technology resources, e.g., installations, personnel, equipment, electronic media, documents, etc., from damage, loss, theft, or unauthorized physical access.

Federal Information Processing Standards (FIPS) Publication (Pub) 31, "Guidelines for ADP/IT Physical Security and Risk Management," provides guidelines to be used by Federal organizations in structuring physical security programs for ADP/IT facilities.

It is MHS policy that:

a. Facility managers prepare physical security plans to include AIS/Network Physical Security.

b. Physical security plans be based on FIPS Pub 31, "Guidelines for Automatic Data Processing Physical Security and Risk Management." No two facilities are alike; therefore, no two plans will be the same. However, the plans must address at least the following areas:

   1) Fire

   2) Water damage

   3) Air conditioning

   4) Electricity

   5) Natural disasters, such as lightning strikes

   6) Access control

   7) Housekeeping

   8) Other considerations, such as bomb threats and civil disturbances

c. Plans be continually enforced, annually tested, and updated, as required.

5.6 Procedural Security

Procedural security is a set of management constraints and supplemental controls established to provide an acceptable level of protection for information. It is synonymous with administrative security and it provides the actions, controls, processes, and plans to ensure continuous operation of an AIS or network within an accredited security posture. It is an integral part of the overall IA environment and supports the concepts of defense-in-depth. Procedural security measures complement technical security measures and can provide alternatives to technical security when risk analysis indicates that the use does not increase the overall risk to an AIS or network. They are site and task dependent.

It is MHS policy that:

a. Procedural security measures be developed by the ISSO/NSO to complement the technical security measures offered by hardware, software, and firmware.

b. Processes such as security training, user access control, media labeling, and SBU information handling be included in the set of measures developed.

c. The Services will follow Service-specific policy for procedural security.

5.7 SECURITY TRAINING AND AWARENESS PROGRAM

Employees must be informed of applicable organizational policies and procedures and will be expected to act effectively to ensure the security of system resources. Initial and periodic user Security training and awareness will ensure all users are aware of security issues and what actions to take when an event or incident occurs.

It is MHS policy that:

a. An IA security training and awareness program will be maintained for all personnel.

b. All users be required to undergo security training upon initial assignment. Thereafter, annual training must occur.

c. Training will be tailored to what the user needs to know to operate the system securely.

d. Initial and annual Privacy Act training will be accomplished in accordance with DoD policy for the protection of privacy information.

e. Individuals must receive refresher training annually to assure that they continue to understand and abide by the rules.

f. The following security areas, at a minimum, shall be addressed during training:

1) Good general security practices

2) Reporting security incidents

3) Threats (sources and impacts) and vulnerabilities overview

4) Computer viruses

5) Password management

6) Proper protection, storage, and disposal of SBU information

7) Internet usage

8) E-mail usage

9) Software use including copyrights and downloading software from Internet Web sites

10) Area security including challenging strangers and escorting unauthorized personnel

g. Security training and awareness will be accomplished in the following ways:

1) Computer Based Training (CBT) via Defense Information Systems Agency's (DISA) Security Awareness compact disk (CD)

2) Pamphlets

3) Classroom Instruction

4) Placing security awareness training material on a network shared drive with the ability to track successful completion of training

5) Training will be documented and maintained to corroborate compliance with policy

h. Security and awareness training should be required of all system users before they are granted access to the system, at least annually, and when significant events affecting the system take place (e.g., a new operating system is installed).

5.7.1 Program Manager (PM) Training

It is recommended that PMs attend the Operational Information Systems Security Course.

The course is sponsored by DISA and is provided free to U.S. military and civilian employees. Classes are held at DISA in Falls Church, Virginia. Course length is five days. The theme focuses on information systems security policies; roles and responsibilities; modes of operation; basic concepts of risk management; contingency planning; C&A; internet connectivity; access controls; auditing; Trusted Computer Systems practices, procedures, and concepts; malicious logic; network security; basic concepts of cryptography; and computer crime.

5.7.2 Information Systems Security Manager (ISSM) Training

It is MHS policy that ISSMs attend the Operational Information Systems Security training course.

The course is sponsored by DISA and is provided free to US military and civilian employees. Classes are held at DISA, in Falls Church, VA. Course length is five days, and the theme focuses on information systems security policy; roles and responsibilities; modes of operation; basic concepts of risk management; contingency planning; C&A; internet connectivity; access controls; auditing; Trusted Computer Systems practices, procedures, and concepts; malicious logic; network security; basic concepts of cryptography; and computer crime.

5.7.3 Information Systems Security Officer (ISSO) Training

Security training for ISSOs will include security policies and procedures in such areas as physical, personnel, software, hardware, administrative, configuration management, communication security, and contingency planning.

It is MHS policy that ISSOs attend the DISA-sponsored Information Security (INFOSEC) course described in the preceding paragraph or obtain the DISA-developed ISSO training CD and take the course via self-instruction.

5.7.4 System Administrator (SA) Training

SA training should be based on the platform and software used to operate the specific server being administered. Training is commonly available from the platform or software vendor and should include background in system security and other networking functions associated with the server to be administered. DISA offers several courses targeted at the System Administrator; some require classroom attendance while others are based on compact disk-read only memory (CD-ROM) technology.

It is MHS policy that:

a. SA training concentrate on security of the system being administered.

b. NSO/SA training on the subject of firewalls will comply with paragraph 5.7.5 below, “Firewall Administrator Training.”

5.7.5 Firewall Administrator Training

Site management should ensure that the designated administrators are available to attend Firewall Training. Prior to designating an individual as a firewall administrator, the site should ensure that the designated individual has a strong background in Windows NT, Microsoft Exchange, Unix, Hewlett Packard (HP) Openview, TCP/IP, DNS, Sendmail, and Cisco routers. In addition, extensive courses are available from training institutions in the following areas:

a. Windows NT Security/Windows 2000 Security as appropriate

b. Overview of firewall components

c. Bastion host configuration

d. Cisco router configuration

5.8 Marking and Labeling

The proper marking and labeling of SBU information and hardware, as required, will help prevent the loss, misuse, or unauthorized access to, or modification of, SBU information.

Sensitive material is information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Title 5, U.S. Code, Section 552a (The Privacy Act), but has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

SBU output should be marked to accurately reflect the sensitivity of the information. The marking may be automated (i.e., the AIS has a feature that produces the markings) or may be done manually. When SBU information is included in DoD documents, it shall be marked as if the information were For Official Use Only (FOUO).

5.8.1 Storage Media

ISSOs and SAs must identify the storage media to be used with a system. Such media must have external labels indicating the security classification or sensitivity of the information. Storage media is classified at the same level as the AIS or network of which it is a part. In addition, the media must display applicable associated security markings, such as handling caveats and dissemination control labels.

5.8.1.1 Removable Media

Removable media will be marked, physically controlled, and safeguarded in a manner prescribed for the highest classification/sensitivity recorded on them until such time as the media is destroyed or sanitized.

5.8.1.2 Non-removable Media

Non-removable media shall bear external labels indicating the security classification/sensitivity of the information and its associated security markings, such as handling caveats and dissemination control labels. If it is not practicable to mark the non-removable media itself, the label will be affixed to the front of the personal computer (PC) or storage media cover.

5.8.2 Marking Hardware Components

Procedures must be implemented to ensure that components of an AIS or network, including input/output devices that retain sensitive information, workstations, terminals, personal computers, standalone personal computers, and word processors used as terminals, bear a conspicuous external label that states the highest classification/sensitivity of information that can be processed on the AIS or network. The notice may consist of either permanent markings or a label.

5.8.3 Privacy and Data Handling

a. Information processed and output (printed) on Tri-Service and contractor AISs and networks shall be treated as follows: All patient information processed by Tri-Service and contractor AISs and networks is SBU and will be protected, marked, or labeled in accordance with DoD policy for the protection of FOUO information.

b. TRICARE beneficiaries have a right to privacy of their information. Accordingly, controls must be established to affect this policy.

c. As required by The Privacy Act, when obtaining information from an individual, a Privacy Act Statement shall be provided to the individual advising of:

    1) The authority for soliciting the information.

    2) The principal purposes for which it will be used.

    3) The routine use to be made of it.

    4) Whether furnishing the information is mandatory or voluntary.

    5) The effect on the individual for not providing the information.

d. Privacy Act data must be labeled as follows:

    1) For Official Use Only.

    2) Warning: This information requires protection under the Privacy Act.

5.8.4 For Official Use Only (FOUO) Material

FOUO material is information that has not been assigned a security classification, but which may be withheld from the public for one or more reasons cited in the Freedom of Information Act (FOIA) exemptions list. DoD 5400.7-R, "DoD Freedom of Information Act Program," provides policy and guidance on this matter.

Printouts and media that contain FOUO information require special handling, storage, safeguarding, marking, and disposal procedures. FOUO messages must be marked appropriately and transmitted in accordance with communications security procedures. Unauthorized disclosure of FOUO information could result in civil and criminal sanctions.

It is MHS policy that:

a. FOUO information will be handled in accordance with DoD 5400.7-R, "DoD Freedom of Information Act Program."

b. FOUO information not be posted on publicly accessible Web sites.

5.9 CONFIGURATION MANAGEMENT

Configuration management is the management and oversight of changes made to a system's hardware, software, firmware, documentation, connectivity, and tests throughout the life of that system. It consists of identifying, documenting, and verifying the functional and physical characteristics of an AIS or network. Moreover, it controls changes to the AIS and network, and the accompanying documentation. Configuration Control Boards (CCB) at the enterprise, program, Service, and facility level, must ensure that changes to an AIS or network do not negate the security countermeasures of the AIS or network.

5.9.1 Configuration Management Policy

It is MHS policy that:

a. No changes to the configuration of an AIS or network will be made until the ISSO evaluates the effect(s) the proposed change will have on the security countermeasures in place on the AIS or network.

b. ISSO approval is required before any configuration changes are made to an AIS or network.

c. The ISSO will ensure configuration changes do not have an adverse impact on the security countermeasures of the AIS or network.

d. During the life-cycle of the AIS or network, a configuration management system be in place for security-relevant hardware, firmware, and software.

e. PMs, ISSOs, and SAs maintain control of changes to the formal model, the descriptive and formal top-level specifications, other design information, implementation documentation, source code, the running version of the object code, and documentation.

f. Tools be available and maintained under strict configuration control for comparing a newly generated version of software with the previous version. These tools must ascertain that only the intended changes have been made in the code that will be used as the new version of the AIS or network.

g. The ISSO document the implementation of a change in the SSAA.

The strategy for managing change must be defined in the SSAA. Detailed guidance exists in National Computer Security Center (NCSC)-Technical Guidance (TG)-006, "A Guide to Understanding Configuration Management in Trusted Systems," and in Military Handbook (MIL-HDBK)-61A, "Configuration Management Guidance."

5.9.2 Configuration Management Plan

A Configuration Management Plan establishes controls for making changes to the AIS and network resources. It includes a list of components, the configuration of the peripherals, and interconnections to other AISs or networks. In addition, items such as version releases of software, information on batch files, and environmental settings for paths and switch settings of machine components are addressed. See **Figure 6**, Configuration Management Plan Content.

CONFIGURATION MANAGEMENT PLAN CONTENT

- Roles and Responsibilities.
- Tools, i.e., forms, labels, automation
- Procedures – routine and emergency
- AIS and Network Components
- Peripherals
- Interconnections to other AISs and Local Area Networks (LANs)
- Description of the baseline, e.g., software versions, batch files, and environmental settings
- Process for keeping the plan current

Figure 6. Configuration Management Plan Content

5.9.2.1 Documentation and Source Code Libraries

Up-to-date information is essential for disaster recovery activities.

It is MHS policy that SAs/NSOs establish and maintain:

a. Documentation of hardware and software configurations and diagrams essential to allow resumption of operations after a hardware/software failure.

b. Clearly identified hardcopy of software source code, libraries, and diagrams essential for recovery operations.

c. The latest version of installed software should be maintained.

Each system is unique; therefore, its Documentation and Source Code Libraries will be unique. ISSOs must keep on hand up-to-date copies of records needed to prevent an extended interruption of service.

Safeguards are critical to prevent unauthorized access to source code libraries.

5.10 CONTINGENCY PLANNING

The Federal government's continued dependence on computers, and the data processed by them, has increased the importance of plans to prevent loss of their availability. Years ago, it was reasonable to consider reverting back to manual operations when AIS or networks became unavailable. Today, there are but few situations in which it is even possible to revert to manual processes. Thus, contingency plans are necessary to minimize the damage caused by unexpected and undesirable occurrences (contingencies) in and about AIS and network facilities.

Security measures are employed to prevent or detect accidental or intentional disclosure, modification, or destruction of data or loss of the means of processing those data. Contingency plans, on the other hand, should be designed to reduce to an acceptable level the consequences of any loss of AIS or network resources or capability; they are not just planned responses to major catastrophes. As stated earlier, the purpose of a contingency plan is to mitigate the damaging consequences of unexpected and undesirable events of *whatever magnitude.* A contingency plan must not be directed exclusively at reaction to catastrophically destructive occurrences. While it is clearly true that those who are responsible for AIS and network resources must plan for the possibility of such catastrophic loss, they must also plan against less-than-cataclysmic events, which also seriously impede AIS and network operations. A contingency plan is a roadmap of action to reduce the consequences of loss of AIS or network resources or capabilities if events occur that prevent normal operations. Contingency plans should be a part of every security program to ensure the availability of critical resources and to facilitate the continuity of operations during an emergency.

The job is not complete as soon as the contingency plan has been written because a plan that has not been tested cannot be assumed to work. Likewise, due to the volatile nature of ADP/IT processing in which the environment is constantly changing, a plan that has been tested only once and then filed away provides a false sense of security.

It is MHS policy that:

a. AIS and network SAs/ISSOs will coordinate the development of contingency plans that address COOPs and DRPs.

b. Management at all echelons, NSOs, ISSOs, and SAs must actively participate in the planning and periodic testing of contingency plans.

c. Contingency plans shall be developed and tested in accordance with guidance contained in the FIPS Pub 87, “Guidelines for ADP/IT Contingency Planning.”

d. Plans must be tested annually under realistic operational conditions.

For additional guidance refer to FIPS Pub 31, “Guidelines for Automatic Data Processing Physical Security and Risk Management.”

5.10.1 Off-Site Storage of System Backup Files

Off-site storage of backup files is the caching of important documents at a location separate from the primary processing site. It can be considered as additional insurance against destruction of the primary processing facility. Catastrophic failures could involve a total loss of computing capability at the primary site. These failures may arise from enemy action or from something as mundane as a fire caused by a careless smoker. Maintaining complete up-to-date copies of AIS software, electronic files, documentation, procedures, restoration plans, and maintenance agreements, and storing them at an off-site location will allow the resumption of operations.

It is MHS policy that offsite storage be addressed in contingency plans, along with the provision of adequate security safeguards to prevent unauthorized access to the information while it resides in storage.

5.11 Incident Reporting and Response

5.11.1 Incident Reporting

Incident reporting is the notification provided to higher and/or lower echelons regarding out-of-the-ordinary events such as intrusions, denials of service, malicious logic attacks, and probes.

MHS sites should have a structured ability to audit, detect, isolate, and react to intrusions, service disruptions, and incidents that threaten the security of operations. Two positions play critical roles in this area. They are the Help Desk and the ISSO.

The Help Desk is the focus because incidents are **reported to** the Help Desk and responses **emanate from** the Help Desk. This is the location that the User/SA calls when an incident out of the ordinary occurs. This is the location that initiates a response to that incident.

The ISSO position is critical because he/she is responsible for ensuring that the entire AIS and network implement the MHS IA provisions stated herein. The Help Desk is included as part of the AIS and network.

The following paragraphs discuss incident reporting and response.

It is MHS policy that:

a. MHS organizations are required to report incidents via the chain of command.

b. The following incidents will be reported to the Help Desk by the SA/ISSO:

    1) Intrusion attacks will be reported by the SA/ISSO.

    2) Denial of service attacks will be reported by the SA/ISSO.

    3) Probes will be reported by the SA/ISSO.

c. All users will report all virus/worm (malicious logic attacks) to the Help Desk.

5.11.1.1 Intrusions

Intrusions are unauthorized accesses to an information system.

5.11.1.2 Denials of Service

Denials of service are actions that prevent any part of an automated system from functioning in accordance with its intended purpose. This includes action that causes the unauthorized destruction, modification, or delay of service.

5.11.1.3 Malicious Logic

Malicious logic is hardware, software, or firmware that is intentionally included in an information system for an unauthorized purpose, such as a virus or Trojan Horse.

5.11.1.4 Probes

Probes are online attempts to gather information about an automated information system or its users.

5.11.2 Incident Response

5.11.2.1 Joint Task Force (JTF), Computer Network Defense (CND)

CND is defined as actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks. The unauthorized activity may include disruption, denial, degradation, destruction, exploitation, or access to computer networks, information systems or their contents, or theft of information.

In accordance with DoDI O-8530.2, “Support to Computer Network Defense (CND)”, and DODD O8530.1, “Computer Network Defense (CND),” the Joint Task Force, Computer Network Defense (JTF CND), an element of Space Command (SPACECOM), serves as DoD’s focal point for CND. The JTF CND provides assistance in identifying, assessing, containing, and countering incidents that threaten DoD information systems and networks. It collaborates and coordinates DoD efforts with other government and commercial activities to identify, assess, contain, and counter the impact of computer incidents on national security communications and information systems, and to minimize or eliminate identified vulnerabilities.

Formal documentation to address CND is being prepared by SPACECOM; when it is implemented, this Manual will be updated. In the interim, SPACECOM has established the JTF CND as the central site from which to launch a defense against attacks on systems.

5.11.2.2 Information Systems Security Officer (ISSO)

ISSOs play an essential role in responding to incidents. They are responsible for ensuring that procedures utilized in incident response actions comply with DoD guidelines providing traditional computer emergency response services.

5.11.2.3 Help Desk

A Help Desk is an easily accessed central point in an AIS and network that is staffed during normal working hours – at some locations, 24 hours a day – to provide timely and efficient technical support to users. The support is wide ranging, covering hardware and software in both operational and system matters. Because of its accessibility and widely accepted role in solving problems, it is a natural channel through which incidents that threaten an AIS and network can be reported.

Help Desks usually fall under the purview of Network Operations. The Manager of Network Operations must publish a Help Desk Standard Operating Procedure (SOP) to ensure that incidents are reported up the chain of command to keep MHS personnel advised of the status of network security. Many incidents can be addressed locally, and in those cases the Help Desk technician will initiate action and follow up procedures until the incident is brought to a satisfactory end. If the complexity of the incident is beyond the Help Desk's capability to address it completely, the Help Desk technician will notify the manager of Network Operations who, if the severity of the incident warrants, will notify the Watch Officer at JTF CND and the TMA Director, Network Operations or appropriate service level designee. The degree of severity is a matter of judgment, so the Manager of Network Operations is expected to exercise rationality.

5.11.2.4 Users

When irregularities occur, users must contact the Help Desk. If the Help Desk is not available and the severity of the incident warrants, call the manager of Network Operations.

5.12 INFORMATION ASSURANCE VULNERABILITY ALERT (IAVA) PROGRAM

A vulnerability is a weakness in an AIS or network that could be exploited, and the IAVA process is a comprehensive distribution method to notify Commanders in Chief (CINC), Services, and Agencies about vulnerability alerts and countermeasures information. As the IAVA process manager, DISA, via its DoD Computer Emergency Response Team (DoD CERT), is responsible for disseminating vulnerability notifications. DISA provides notification and monitoring services of technical information associated with Information Assurance Technical Advisories (IATAs), Information Assurance Vulnerability Alerts (IAVAs), and Information Assurance Vulnerability Bulletins (IAVBs) to the MHS. These notices may include information about implementing patches and network upgrades in response to viruses, new vulnerabilities, malicious hacker attacks, and other similar intrusions.

Appendix E of this Manual, *MHS Information Assurance Vulnerability Alert (IAVA) Process*, outlines procedures for IAVAs within the MHS.

5.13 VULNERABILITY ASSESSMENT SOFTWARE

Vulnerability assessment software can identify weaknesses in an operational environment, validate a site's overall security posture and degree of system integration, and usually provide recommendations on ways to address shortcomings. Commercial-off-the-shelf software (COTS) products are available to assist the SA in assessing the vulnerability of an AIS and network. They have the capability to inspect an AIS/network for binary file modifications, vulnerable system versions, weak passwords, vulnerabilities from security misconfigurations, and change detection on files and directories. Government off the shelf vulnerability assessment software is also available from DISA free of charge to all U.S. Government agencies.

5.13.1 Defense Information Systems Agency (DISA) Vulnerability Assessment Software

The vulnerability assessment software products listed below can be obtained from DISA:

a. Security Profile Inspector (SPI) for Windows NT (SPI-NT)

b. Security Profile Inspector (SPI) for Unix Networks (SPI-NET)

The SPI can be downloaded from: http://www.CERT.MIL/resources/security_tools.htm

It is MHS policy that:

a. The SA/ISSO obtain and run vulnerability assessment software on AISs and networks monthly.

b. Vulnerability assessment software will only be run during periods of low network usage (i.e. weekends).

5.13.2 Penetration Testing

> *"Since penetration testing is designed to simulate an attack and use tools and techniques that may be restricted by law, Federal regulations, and organizational policy, it is imperative to get written permission for conducting penetration testing prior to starting."*
>
> NIST Special Publication 800-42, "Draft Guideline on Network Security Testing"

Penetration Teams have the ability to identify, and take advantage of (penetrate) AISs and network vulnerabilities, and to make recommendations as to what countermeasures should be used to mitigate or eliminate vulnerabilities.

The MHS Penetration Team is an independent threat-based activity aimed at readiness improvements through simulation of an opposing force. The MHS Penetration Team is a friendly force that matches an adversary's approach to an attack by performing penetration testing. The MHS Penetration Team normally performs penetration testing during the C&A process for an AIS or network. However, their services may be requested by an AIS owner or manager to verify the security mechanisms of their AIS or network. Requests for penetration testing should be sent to the MHS IA Program Office.

Penetration services are also available from the DISA Field Security Office and the National Security Agency (NSA).

It is MHS policy that:

a. AIS and network owners are authorized to request MHS Penetration Team support to verify adequacy of security counter measures in place.

b. Requests for MHS Penetration Team support, or support requested from an outside agency, must be coordinated through the MHS IA Program Office.

c. MHS Penetration Team activities be controlled at the highest level of management.

d. The MHS C&A team does not conduct penetration tests at a military treatment facility (MTF) unless requested to do so.

5.14 Risk Management

Risk management is the process of identifying, measuring, controlling, and minimizing or reducing the security risk incurred by an AIS or network to a level commensurate with the value of the assets protected. It includes risk analysis, cost benefit analysis, selection, implementation and testing of security mechanisms, security evaluation of safeguards, and overall security review. Identifying threats to an AIS or network and determining the vulnerabilities that may be exploited by the threats is accomplished to ensure an acceptable level of security is achieved. PMs and security personnel must develop countermeasures to eliminate or reduce vulnerabilities to an acceptable level.

5.14.1 Risk Assessment

Risk assessment is the process of analyzing threats to, and vulnerabilities of, an AIS and network and the potential impact that the loss of information or capabilities of a system would have on national security. It appraises the operation of the system to determine if the risk to availability, integrity, authentication, confidentiality, and non-repudiation is being contained or reduced to an acceptable level. The resulting analysis is used as a basis for identifying appropriate and cost-effective security countermeasures.

Assessing risk is an ongoing activity, which ensures that new threats and vulnerabilities are identified and that appropriate security countermeasures are implemented. Methods should include a consideration of the major factors in risk management: the value of the AIS and network or application, threats, vulnerabilities, and the effectiveness of current and proposed safeguards. A risk assessment will be performed annually to identify potentially new vulnerabilities and to verify current security safeguards continue to provide adequate protection.

5.14.2 The Program Manager’s (PM's) Role in Risk Management

PMs are responsible for ensuring risk management is accomplished in the acquisition arena. The DoD Risk Management Web site, http://www.acq.osd.mil/io/se/risk_management/index.htm, clearly identifies risk management as a PM responsibility.

5.14.3 MHS Risk Management Policy

It is MHS policy that:

a. A risk management process will be implemented by PMs, contractors, and ISSM/ISSOs to enhance security of AISs and networks under their purview.

b. PMs, ISSM/ISSOs, and contractors must conduct risk assessments at least annually.

c. PMs, ISSM/ISSOs, and contractors establish risk management processes that include:

    1) Planning for risk management.

2) Continuously identifying and analyzing program events.

3) Assessing the likelihood of the occurrence of an event and the consequences.

4) Incorporating handling actions to control risk events.

5) Monitoring a program's progress toward meeting program goals.

5.14.4 Risk Management Publications.

The following documents provide guidance on how to perform Risk Management/Analysis:

a. NCSC-TG-024-1, "A Guide to the Procurement of Trusted Systems" (Purple Book), contains guidance for the management of risk.

b. FIPS Pub 191, "Guideline For the Analysis of Local Area Network Security."

c. NIST Special Publication 800-12, "An Introduction to Computer Security."

d. DoD 8510.1-M, "DITSCAP Application Manual."

e. Navy IA Publication 5239-16, "Risk Assessment Guidebook," located at https://infosec.navy.mil/SERVICES/.

f. ISO/IEC 12207, Software Life Cycle Processes.

5.15 FEDERAL ETHICS FOR USE OF THE INTERNET AND E-MAIL

DoD 5500.7-R establishes Federal ethics for use of the Internet. The MHS may provide civilian employees and assigned military personnel, temporary workers, independent contractors and agents with access to the Internet to perform assigned business functions. MHS Internet connections are government property. Personnel do not have a privacy interest in using them. The MHS may monitor Internet use by automated means or human intervention, at its sole discretion, in the ordinary course of business, at any time, with or without notice. The MHS may employ software to protect employees from inappropriate material and reserves the right to block access to these sites at any time, for any reason.

It is MHS policy that:

a. Internet/e-mail systems and commercial systems paid for by the Federal Government shall be for official use only and authorized purposes only.

b. Official use includes emergency communications and communications that are necessary in the interest of the Federal Government.

c. Authorized purposes include brief communications made by DoD employees while they are traveling on Government business to notify family members of official transportation or schedule changes. They also include personal communications from the DoD employee's usual work place that are most reasonably made while at the work place, such as checking in with spouse or minor children; scheduling doctor and auto or home repair appointments; brief internet searches; and/or e-mailing directions to visiting relatives when such communications:

1) Do not adversely affect the performance of official duties by the DoD employee or the employee's organization.
2) Are of reasonable duration and frequency, and whenever possible, made during the employee's personal time, such as after duty hours or lunch periods.
3) Serve a legitimate public interest, such as keeping employees at their desks rather than requiring the use of commercial systems; educating the employee on the use of the communications system; improving the morale of employees stationed for extended periods away from home; enhancing the professional skills of the employee; and/or job-searching in response to Federal Government downsizing.
4) Do not put Federal Government communications systems to uses that would reflect adversely on DoD or the MHS, such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violations of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service.

d. Incidents of unauthorized activity or misuse or abuse of the Internet or e-mail use may be investigated and the perpetrator could be subject to disciplinary action and/or monitoring action as appropriate.

e. Patient information is one of the categories defined by DoD as FOUO information and will not be sent via e-mail unless the appropriate security controls are in place.

5.16 MHS Information Assurance Working Group (IAWG)

The MHS IAWG is a working-level body tasked to ensure that the MHS maintains a high level of Information Assurance (IA) for centrally managed Automated Information Systems (AISs) and Networks. The signed MHS IAWG Charter is provided as Appendix G. Voting members of the IAWG include representatives from the Army, Navy, and Air Force Surgeons General offices, Program Executive Office, and TMA directors will have the occasion to provide the MHS with comments and recommendations regarding the draft or revised policy.

5.16.1 MHS IAWG Functions

The MHS IAWG shall perform the following functions:

a. Evaluate, review, and make recommendations on IA issues for all MHS activities and organizations to the Technical Integration Working Group (TIWG) and the Information Management (IM) Program Review Board (PRB).

b. Facilitate the exchange and sharing of IA information among the Army, Navy, Air Force, DoD, Department of Veterans Affairs, MHS Program Office Managers, and external partners.

c. Review Services, DoD, and Federal IA policies and guidance, and other security-related issues, and determine impact to the MHS.

d. Develop implementation criteria for MHS IA Program Offices to address new IA policies, procedures, and technologies mandated by DoD.

e. Monitor the IA status of MHS programs and policies for compliance with Federal and DoD security regulations.

6.0 TECHNICAL INFORMATION ASSURANCE

6.1 OVERVIEW

Technical IA is the act of applying the proper security configuration to network components, such as routers, firewalls, network management workstations, IDSs, communications devices, ports and protocols; server operating systems; and security services. Technical IA safeguards are implemented by SAs, NSOs, and ISSOs. The implementation of technical IA is essential for the protection of AISs and networks and SBU information against malicious code (viruses), and hacker attacks such as Denial of Service (DoS), and interception/theft or modification of sensitive information. The improper implementation of technical safeguards by untrained personnel could result in a disruption of service or network operations. Technical personnel should receive adequate training before attempting to implement technical IA safeguards. For AIS and network accreditation, DoDI 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," mandates specific security requirements be implemented and maintained for AIS and networks during all aspects of design, development, deployment, operation, and maintenance. The Defense Department has published additional technical IA policy, which complements the DITSCAP requirements, and are a result of lessons learned, research, testing, and best of breed security practices.

It is noted that the DoD is currently developing a Ports and Protocols Policy document. Upon finalization of the policy, this Manual will be updated.

6.1.1 SECURITY CONFIGURATION GUIDELINES

The National Security Agency has developed Security Recommendation Guides for operating systems and routers that should be consulted to maximize security features of systems and equipment. As an example, the Systems Administration Guidance for Windows 2000 Professional publication is intended to assist the users and system administrators of Windows 2000 Professional systems in configuring their hosts by providing configuration templates and security checklists. The guide provides detailed information about the security features of Win2K Pro, security configuration guidelines for popular applications, and security configuration guidelines for the Win2K Pro operating system. The guide documents the methods that the system administrators can use to implement each security setting. The principal goal of the document is to recommend and explain tested secure settings for Win2K Pro workstations with the objective of simplifying the administrative burden of improving the security of Win2K Pro systems.

6.2 NETWORK INFRASTRUCTURE

Network infrastructure is composed of communications closets, communications devices, wiring, PCs, and workstations. DoS is considered one of the easiest attacks on an infrastructure. Power can be interrupted, wires cut, and communications devices turned off. Attacks on network infrastructure include capturing data, manipulating data and reintroducing it onto the network, and replaying attacks. Protecting the infrastructure is not limited to a single scope, but must be a total protection effort. To effectively apply these security measures to the MHS network infrastructure, due consideration must be applied to the Open System Interconnection (OSI). The OSI network model is divided into seven layers. They are as follows:

a. First: Physical Layer

b. Second: Data-Link Layer

c. Third: Network Layer

d. Fourth: Transport Layer

e. Fifth: Session Layer

f. Sixth: Presentation Layer

g. Seventh: Application Layer

6.2.1 Physical Layer Security

The physical layer is the medium over which information travels. The medium could consist of copper wires, fiber optic cables, and wireless transmissions. It also includes the equipment that connects hosts to the medium (e.g., transceivers, NIC, and taps). Securing and maintaining this portion of the network infrastructure is crucial to an effective security plan.

6.2.1.1 Cables and Components

It is MHS policy that all ISSOs/NSOs will be familiar with the cable technology used within the sites and the associated risks.

6.2.1.2 Data outlets

It is MHS policy that the ISSO and NSO will ensure all data outlets not in use are detached and/or disabled from the network infrastructure in the communications closet. This will prevent the communications device from accepting a packet on a given port, even if a piece of equipment, such as a laptop or sniffer, is connected to that port.

6.2.1.3 Topology

It is MHS policy that the ISSO and NSO will be familiar with the LAN topology used within the sites and the limitations and security implications.

6.2.1.4 Cable Management

It is MHS policy that:

a. The ISSO/NSO will maintain a current drawing, or as-builts, of the network under the ISSO/NSO's control. The drawing should include all remote connections, all local connections to domains not under site control, and all internal connections to PCs/workstations, servers, routers, bridges, and switches. Cable routes should be annotated and any special circumstances concerning the installation, such as a path that leaves a controlled environment, should be noted.

b. The ISSO/NSO will periodically run HP Openview and will review the results for the presence of unauthorized devices.

c. All communications lines will be labeled and documented to show destination and source within the physical domain of an entity's infrastructure.

d. Major cable runs supporting critical systems will include spares to alleviate potential downtime. If one cable is damaged, the alternate cable can be readily attached. (Spare cables should be fabricated and readily available for installation.)

e. Facility cables (including leased lines) will be protected by routing and/or enclosing them in acceptable distribution hardware (i.e., trays, ducts, etc.).

f. All cable paths will be run within a controlled access area and, wherever possible, always under the site's control. If cables are run in areas not under the site's control, a memorandum of understanding (MOU) should be established between the sites and the controlling authority responsible for the structure supporting the cable run.

NOTE: In this case, **controlled access area** means controlled restriction to authorized site personnel.

6.2.1.5 Installation Standards

It is MHS policy that the following installation standards will be complied with:

a. Electronic Industry Association/Telecommunication Industry Association (EIA/TIA)-568, "Commercial Building Telecommunications Standard."

b. EIA/TIA-569, "Commercial Building Standard for Telecommunications Pathways and Spaces."

c. TIA/EIA-606, "Administration Standard for the Telecommunications Infrastructure of Commercial Buildings (American National Standards Institute [ANSI]/TIA/EIA-606-93)," (Feb.1993).

ISSOs/NSOs will ensure all wiring and communications device installations comply with the standards listed in the above bullets.

6.2.2 Switches and Hubs

The common method of infrastructure wiring today is the star topology. Using this convention, all wires are run from a central point (usually a communications closet or computer room) out to each work area. The resulting concentration of wires is connected to an electronic device that electrically functions as a hub. Historically, hubs have been the central points of communications and connectivity to and throughout Medical Treatment Facility LANs. Although hubs are still in use at a number of locations, they are no longer primary edge concentration devices. Switches are now the central points of communications and connection to and throughout the LAN. The MHS is in the process of replacing hubs with switches in conjunction with MTF LAN upgrades.

It is MHS policy that the following guidelines are applicable to concentrator locations:

a. Installation of switches and hubs will be in dedicated locked communications closets. In the case where communications closet access cannot be secured, switches and hubs will reside in locked cabinets.

b. Installation of communications closets/cabinets will be in centralized locations and not along outside walls where they could be vulnerable to electronic eavesdropping from outside the building.

c. The ISSO/NSO will control the keys to the locked dedicated communications closets and cabinets, and will only provide the keys to authorized network personnel and/or network security personnel.

Warning: Installing communications devices such as switches, or hubs in common work areas, even within the controlled access area, leaves them susceptible to disconnection damage that can lead to denial of service.

6.2.2.1 Concentrator Management

It is MHS policy that:

a. The ISSO/NSO will ensure the maintenance sections of the concentrator, switch, or hub are password protected for both viewing and modification.

b. The ISSO/NSO will ensure any initial passwords assigned by the manufacturer will be changed.

6.2.2.1.1 In-Band Management

It is MHS policy that:

a. ISSOs/NSOs will take extreme caution when using in-band management on concentrators. If provided by the vendor, ISSOs/NSOs should use password encryption or a message digest to secure the password and validate the user making the changes. If security provisions are not available, change the password immediately after in-band access.

b. ISSOs/NSOs will ensure the use of in-band management will be restricted to a limited number of authorized internet protocol (IP) addresses.

c. **NOTE: Limited number** would indicate a manageable number (less than ten).

d. When in-band management is used, Access Control Lists, in conjunction with user authentication, will be employed to limit from where devices can be managed and who can access devices.

e. If possible, Telecommunications Network (Telnet) will be restricted by IP address and access control list.

6.2.2.1.2 Out-of-Band Management

Although out-of-band management is considered a secure access technique, it is impractical for managing wide area devices due to the geographical distances involved and centralized management of devices. In addition, most hosting facilities do not allow dial-in for out of band management of devices.

It is MHS guidance that the direct connection out-of-band management method for communications device management should be used whenever possible.

6.2.2.1.3 Port Management

It is MHS policy that if port management services are available on the concentrator or communications device, the ISSO/NSO will activate them on all port connections.

6.2.3 Switches

A switch is a hardware device that provides network accessibility or connects two LANs or LAN segments together. They examine the destination Media Access Control (MAC) addresses of packets before deciding whether to forward the packet to the appropriate port on the switch, an adjacent LAN, or discard it. It compiles and maintains a table of valid MAC addresses and only those addresses in the table will be allowed access to the adjacent LAN. Most switches operate at layer two of the OSI model; the data link layer. Core switches operate at layer three; the network layer.

It is MHS policy that the ISSO/NSO will ensure sites establish filters so that the system handles only those packets derived from authorized MAC addresses. The ISSO should ensure that MAC address filtering is turned on at each access point. Note that MAC address filtering may not be practical for large WLAN implementations.

6.2.3.1 Switch Management

Switches have a console service port to which the NSO or ISSO can connect a terminal or laptop with terminal emulation and configure settings. When a switch has an IP address assigned to it, the switch administrator can establish a Telnet session to it and configure parameters via the LAN.

It is MHS policy that:

a. The NSO/ISSO/SA will ensure passwords are assigned to all switches. Different passwords will be assigned to the differing levels of access, and passwords will be created using accepted password generation schemes (e.g., not words found in the common English dictionary, names, etc.).

b. NSO/ISSO/SA will ensure the initial passwords assigned by the manufacturer are changed immediately. These default passwords must be changed on all accounts.

6.2.4 Bridges

It is MHS policy that:

a. The ISSO/NSO will ensure sites establish filters so that the system handles only those packets derived from authorized MAC addresses.

b. The ISSO/NSO will ensure the bridge is configured to filter and audit unauthorized packets attempting to pass through the bridge.

6.2.4.1 LAN Address Spoofing

It is possible to logically change or spoof the MAC address of the Network Interface Card (NIC) installed in a PC or workstation with software freely available in the public domain. Doing so allows unauthorized devices access to LAN segments beyond the bridge, even if MAC layer filtering is enabled.

It is MHS policy that:

a. To combat MAC address spoofing, the ISSO/NSO will maintain a listing of valid MAC addresses, conduct auditing, and review of MAC addresses.

b. The ISSO/NSO will establish a policy stating that only authorized personnel will use NIC software utilities.

If only one or two types of NICs are installed, a check of the various organizationally unique identifiers (OUIs) on the LAN can assist in keeping the NSO informed of unauthorized devices, such as sniffers, connected to the LAN. Auditing systems should be configured to track, record, and alert for any unknown MAC addresses identified on the network.

6.2.4.2 Bridge Management

Bridges have a console service port to which the NSO or ISSO can connect a terminal or laptop with terminal emulation and configure the bridge settings. In addition, the bridge might have an IP address assigned to it, with which the bridge administrator can establish a Telnet session and input settings via the LAN.

It is MHS policy that:

a. NSO/ISSO/SA will ensure out-of-band management will be used for all bridge management commands. In-band management will be limited to emergency situations, and the password will be changed immediately after in-band access.

b. NSO/ISSO/SA will ensure passwords are assigned to all bridges. Different passwords will be assigned to the **view** option and the **write** option portions of the bridge, and passwords will be created using accepted password generation schemes (e.g., not words found in the common English dictionary, names, etc.).

c. NSO/ISSO/SA will ensure the initial passwords assigned by the manufacturer are changed immediately.

6.3 WIDE AREA CONNECTIVITY

The purpose of the following sections is to outline security practices covering interconnection devices. These devices connect LANs to LANs, LANs to WANs, and LANs and workstations to remote services. The following subsections set guidance that applies to all communications devices.

6.3.1 Passwords

An automated password generator creates random passwords that have no association with a particular user. Passwords used for the protection of communication devices should be in accordance with FIPS PUB 181, “Automated Password Generator (APG) Standard.” The APG Standard specifies an algorithm to generate passwords for the protection of computer resources. This standard is for use in conjunction with FIPS PUB 112, “Password Usage,” which provides basic security criteria for the design, implementation, and use of passwords. The algorithm uses random numbers to select the characters that form the random pronounceable passwords. The random numbers are generated by a random number subroutine based on the Electronic Codebook mode of the Data Encryption Standard (DES) (FIPS PUB 46-1).

It is MHS policy that:

a. All communications devices will be password protected.

b. All default manufacturer passwords will be changed.

c. All known backdoor User-IDs and passwords will be removed.

d. Strong password usage or password generators will be used to protect communication devices.

e. The ISSO or NSO will record the passwords used on communications devices and store them in a secure or controlled manner.

f. The ISSO or NSO will change the password immediately and restrict by IP address if in-band or remote management is required.

6.3.1.1 Device Management

It is MHS policy that:

a. The NSO will manage devices through direct connection (e.g., out-of-band or direct connection).

b. The NSO will limit the use of remote or in-band management to emergency situations on a case-by-case basis

c. One-time passwords will be changed after use.

d. The NSO will protect image files loaded via the Trivial File Transfer Protocol (TFTP) process from corruption and will be checked on a weekly basis and will be disabled when not in use.

e. The NSO will ensure that communications between devices and the TFTP server are as secure as possible. At a minimum, this should be accomplished by restricting communication to known authorized IP addresses.

f. The NSO will disable all ports except those needed to support the mission of the sites.

6.3.1.2 Warning Banners

The purpose of the warning banner is two-fold: It is like an electronic ***No Trespassing*** sign that provides a legal basis for prosecuting those who disregard the warning and actually do trespass. Secondly, it warns both authorized and unauthorized users that they are subject to monitoring to detect unauthorized use. This provides the informed consent that again allows for a legal basis to prosecute those who abuse the system.

It is MHS policy that:

a. Warning banners will be deployed on all network devices allowing Telnet, File Transfer Protocol (FTP), or Hyper-Text Transfer Protocol (HTTP) access.

b. The banner should be installed so that it appears before a logon screen or before any identification of the system.

c. An escape should also be provided to allow the individual to end the logon attempt (e.g., *Press Enter To Logon To System Or Escape To Abort Session*).

d. If the banner cannot be installed before the logon process due to the configuration of the system, install the banner as soon as possible.

6.3.2 Non-classified (but Sensitive) Internet Protocol Router Network (NIPRNet)

Positive control of all NIPRNet-Internet connections is an absolute requirement. The MHS uses the OSD domain, and it is OSD policy to terminate all unauthorized NIPRNet-Internet connections. This policy was developed to protect the security, availability, and integrity of the NIPRNet from vulnerabilities related to external attacks. To this end, all MHS connections to the NIPRNet will comply with the DITSCAP process and be approved via the NIPRNet connection approval process (CAP). A Web-based interface shall be used to comply with the CAP requirement.

It is MHS policy that:

a. All existing NIPRNet CAP registrations are to be kept up to date by the appropriate circuit Point of Contact.

b. All new telecommunications requirements for NIPRNet connectivity be routed through the TIMPO Circuit Management Office.

c. New NIPRNet circuits will have their systems accredited and registered with the NIPRNet CAP Web site prior to circuit activation.

6.3.3 Leased/Dedicated Lines

Leased lines usually carry an aggregate amount of data, and if unauthorized access were achieved a greater potential for harm could result.

It is MHS policy that:

a. The distance from the LAN to the leased line point-of-presence (POP) will be as short as possible, making the aggregate LAN traffic segment easier to protect.

b. The cable plant should comply with EIA/TIA (568, 569, 606) or applicable FIPS publications.

c. Leased communications lines should be in a protected environment until they reach the Local Exchange Carrier (LEC) POP.

d. When not in routine use, all modems connected to Channel Service Units (CSUs)/DataService Units (DSUs) will be disabled or disconnected.

e. All circuits will be documented. Commercial circuits will be documented with Commercial Circuit System Designators (CCSDs), the LEC ID, and the long haul circuit ID.

6.3.4 Backdoor Circuits

Backdoor circuits are normally those that are connected directly to an internal LAN segment. However, backdoor circuits do not need to be directly connected to the LAN segment. If one organization connects to the LAN properly (e.g., through a firewall or a router with access control lists), but then connects itself to the Internet via an Internet Service Provider (ISP) without the LAN owner's knowledge, a significant security vulnerability exists that could allow attackers unchecked access to the LAN. This type of connection creates a potential hole or *backdoor* to the system, circumventing security. It is for this reason that Government-owned, network-connected computers are not to be authorized direct ISP connections. Cable maps and infrastructure diagrams assist in discovering connections made without permission of the ISSO or NSO.

It is MHS policy that:

a. If Non-Secure Internet Protocol Router Network (NIPRNet) access redundancy is required, it will be accomplished through the use of a Defense Information System Network (DISN) Data Services Server Access Card.

b. Direct connections to a commercial ISP are not authorized.

c. All infrastructure diagrams will be kept up-to-date to show all external connections before actually connecting them. This will show the impact as it relates to all components on the LAN. These diagrams should be based on a physical or automated inspection of the network wiring plant.

d. The ISSO or NSO will investigate all undocumented network connections discovered during any inspection. Unjustified connections should be disconnected.

NOTE: Unjustified connections are those not required or authorized for mission accomplishment.

e. The ISSO or NSO will review all connection requirements on a regular basis to ensure the need remains current. Disconnect any connections that are not fully justified.

f. The ISSO or NSO will monitor all TCP/IP by utilizing an intrusion detection system.

6.4 Routers

Routers provide a seamless path for the forwarding of data from a node on one network to a node on another network. The networks may be collocated or separated by thousands of miles. It is easy to overlook them. They create the openness upon which information sharing is based.

6.4.1 Network Layer Addressing

It is MHS policy that:

a. SAs will distribute, record, and monitor the use of each IP address assigned to any private network in accordance with Request for Comments (RFC) 1918.

b. The ISSO/NSO will ensure that Network IP addresses are current for all networks.

6.4.1.1 Routing Packets

It is MHS policy that:

a. Sites using Cisco routers must use a release of Cisco router software later than Release 11.1, as noted in DoD-CERT Bulletin 93-13.

6.4.1.2 Accessing the Router

It is MHS policy that:

a. NSO/SAs/ISSOs should use RADIUS or the Terminal Access Controller Access System (TACACS) servers, for administrative access.

b. A user-based authentication system be implemented through the use of the **username** command (i.e., **username name password secret**).

c. Routers will be located in a secure room with limited access. The ISSM/ISSO will have ultimate authority to determine who has access to the router, both physically and administratively.

d. The NSO/ISSO will ensure all access points (ports) have passwords, regardless of functionality or the lack thereof (e.g., console, auxiliary, Virtual Terminal [VTY], or line).

e. NSO/ISSO will ensure that the timeout for unattended console and Telnet ports is set for no longer than 15 minutes via the **exec-timeout** command. Activating this timeout feature for an unattended console or for Telnet sessions provides additional security.

f. NSO/ISSO will ensure that all router levels (privileged and non-privileged alike) are password protected. Strong password usage or password generators will be created using password generation schemes.

g. The NSO/ISSO site will change the vendor-provided password. These passwords are well known in the hacker community.

h. It is recommended that NSOs and ISSOs use out-of-band management for all router management commands, limit in-band management to emergency situations, and change the password immediately after in-band access.

i. ISSOs and NSOs who routinely use in-band management for routers will exercise extreme caution. If provided by the vendor, ISSOs/NSOs should use password encryption or a message digest to secure the password and validate the user making the changes. If security provisions are not available, change the password immediately after in-band access.

j. The NSO/ISSO will restrict virtual connections to all network routers by IP address through the use of the **access-class** command.

k. The NSO/ISSO will use the **password encryption** option on the equipment configuration. By default, most routers show the password in clear text to privileged users or to anyone performing a **write** or **show** command. The password encryption command, will encrypt user mode and enable passwords. The router will not show the password in clear text using password encryption. The Cisco Internet Operating System (IOS) software command is **service password-encryption.**

WARNING: Using password encryption will not permit password recovery on some older versions of operating system software. The ISSO will control passwords when using the option.

l. The NSO/ISSO will ensure that access to the router is commensurate with a user's requirements. Those users who have a validated **read** and or **write** requirement will be granted **read** and or **write** authority. Those users who have only a read-specific requirement will be granted **read-only** authority.

m. The NSO/ISSO will disable the **IP alias** command if this is an option. Keeping this enabled allows TCP connections to any port.

n. The NSO/ISSO will limit sensitive areas of the router (i.e., routing tables, access control lists, etc.) to authorized individuals. A person outside the chain of accountability should record these top-level users and their passwords in the event that one of these privileged users no longer has access requirements. This precludes a single individual from denying authorized users necessary access by not telling them the password or by changing it to something unknown.

o. The NSO/ISSO will implement the appropriate audit-related Remote Monitoring (RMON) functions on the router to be used in conjunction with an audit repository system.

p. The NSO/ISSO will audit and record all changes regarding settings, changes, and enhancements. The router will be configured to alarm a Simple Network Management Protocol (SNMP) system for each such occurrence.

6.4.1.3 Access Control Lists (ACLs)

It is MHS policy that:

a. The NSO will set up ACLs to restrict traffic to only that which is required to pass through the site.

b. All unauthorized traffic will be audited and recorded for further investigation.

6.4.1.4 Routing Tables

It is MHS policy that:

a. The NSO will ensure that only required protocols are configured on the router.

b. The NSO will restrict traffic only to known routers.

c. The NSO will audit and alarm for unknown routers attempting to protocol handshake.

6.4.1.5 Router Change Management

People and organizations are forever moving and changing work locations. This sometimes requires updates to router tables.

It is MHS policy that:

a. All router changes and updates will be documented in a manner suitable for review.

b. Request forms will be used to aid the audit trail of any changes to the router requested of the ISSO or NSO.

c. Changes and modifications to routers will be audited by the ISSO so that they can be reviewed.

d. Current configurations of routers will be maintained in a secure location.

e. Router configurations will be copied to a TFTP server for backup.

f. Only authorized personnel will be allowed to request changes to routing tables or service parameters.

Note: The Point-of-Contact (POC) for each router is usually recorded with the domain registration authority for troubleshooting purposes. However, this can open up the change request process to possible spoofing. A person can impersonate the authorized POC and request updates that can deny or stop services altogether.

6.5 COMMUNICATIONS SERVERS

Communications servers allow access to a network infrastructure by various asynchronous devices, such as terminals, printers and PCs, access to a network infrastructure. This access is at the physical layer and provides the connected device the same level of access as any directly attached device. Communications servers usually have one connection to the network and multiple incoming ports connected to modems. These modems can handle dial-up calls or dedicated lines from remote sites. Devices local to the communications server can be directly attached via null modem cables or specially configured cables. Communications servers usually run a protocol such as Point-to-Point Protocol (PPP) or Serial Line Internet Protocol (SLIP) to communicate with the device on the distant end.

Design of a dial-in capability via modems is discouraged for MHS systems and may prevent the system from being deployed to all locations and the Services. Modem use on networks should follow requirements outlined in the Manual and should include dial-back service whenever possible.

6.5.1 Communications Server Access

To ensure a device can communicate with a communications server, it must use and understand a predetermined protocol. This can be a simple signal-level standard such as Recommended Standard (RS)-232C, or the signals can be supplemented with a high-level protocol using compression and authentication such as PPP. Using RS-232 is sufficient for dumb devices such as printers or locally installed terminals. Leaving communications server ports connected to modems configured for no upper layer protocol is an open invitation to unauthorized use. Instituting an upper-layer protocol provides additional identification and authorization to gain access to the network.

It is MHS policy that all private IP address assignments will be in accordance with RFC 1918.

6.5.2 Communications Server Management

Some communications servers require the use of an image file to supply operating parameters and setup configuration. This file can be loaded from a console or via the TFTP process. The address of the TFTP server is coded into the communications server. Whenever it loses the setup and configuration information (such as after a power outage), the communications server downloads the image file to restore service. This server and the TFTP directory must be protected. If an unauthorized user can access the image file and corrupt it, that is the same as having access to the communications server itself. The TFTP by design is an open environment, so it is rather difficult to secure the process, but the data can still be secured.

TACACS and newer versions, TACAS+, are databases that are used by a device such as a router. TACACS/TACAS+ operate using two components, the client code and the server code. These servers operate on a UNIX-based system connected to the router through the out-of-band network. The client protocols allow the router to communicate with the server and to authenticate users.

It is MHS policy that:

a. TACACS/TACAS+ or RADIUS server should be used in conjunction with all communications servers.

b. The NSO/ISSO will maintain a fingerprint of the TFTP image file in an off-line storage media (such as a diskette) and compare them often, especially before reloading the image.

c. The NSO/ISSO will ensure that all levels of the configuration within the communications server are password protected.

d. The NSO/ISSO will ensure that all access points (ports) have passwords, regardless of functionality or lack thereof (e.g., console, auxiliary, or VTY).

e. The NSO/ISSO should restrict access to known authorized traffic between the communications server and the TFTP server.

f. The NSO/ISSO will change all default passwords.

g. The NSO/ISSO will remove all vendor backdoors.

h. The NSO/ISSO will perform configuration using an attached console or out-of-band control. Device management will not be allowed over incoming phone lines that support users. Also, avoid using in-band management over the network. In-band management should be avoided unless absolutely necessary.

i. If the system default is an open system, the NSO/ISSO will assign a password for logon access.

j. The NSO/ISSO will assign passwords to all systems. Different passwords will be assigned to the **view** option and the **write** option portions of the communications server. Passwords will be created using accepted password generation schemes (e.g., password generators).

k. The NSO/ISSO will deploy SNMP so that alarms, warnings, and traps will be detected and reported.

l. The NSO will use Automatic Number Indicator (ANI) options if this function is available. The NSO, or authorized security personnel, will maintain ANI logs in a manner prescribed by the ISSO. This will record all calls for audit trail. Information such as this should be coordinated with those responsible for the operation of the site’s telephone equipment.

6.6 MULTIPLEXERS AND MODEMS

6.6.1 Physical Protection

It is MHS policy that:

a. All modems will be physically protected to prevent unauthorized device changes. If an unauthorized person has physical access to a site’s modems, the switch settings can be changed to affect the security of a system.

b. The ISSO or NSO will maintain a listing of all modems by model number, serial number, associated telephone number, and location. Only Government-authorized modems will be installed in the sites.

c. All multi-user modems and/or modems accessible via the network will be located within the controlled access area of the site or facility. This is an area afforded entry control at a security level commensurate with the operational requirement. This protection will be sufficient to protect the equipment from unauthorized personnel.

d. All modems designed for rack mounting in equipment racks or cabinets will be mounted and physically grounded.

e. Modem connections **will not** be allowed from individual desktop computers that are connected to the AIS and network. The security mechanisms found in software packages running on desktop computers are often inadequate and easily disabled, thereby providing a security vulnerability or back door to the network.

6.6.2 Phone Line Connections

It is recommended that all modems be connected to approved lines using the switched voice network or approved leased lines maintained under Government contract.

It is MHS policy that:

a. All modem phone lines will be restricted and configured to their mission required purpose (inward dial only or outward dial only).

b. All modem phone lines will be restricted to single-line operation without any special features such as the call forwarding capability.

c. ANI will be used if this function is available. The NSO/ISSO will maintain and review ANI logs. These records should be kept for the previous twelve months.

d. The use of personal modems to connect to government phone lines is prohibited unless authorized by the agency’s phone line manager.

6.6.3 Securing Multiplexers

Because multiplexers are not suited for use in an administrative or work area, it is unlikely that one will be attached to a user's PC. Therefore, all instructions and guidelines are based on that scenario.

It is MHS policy that:

a. The ISSO/NSO will ensure that the patch and test facility is in an area that is afforded entry control at a security level commensurate with the operational requirement. This protection will be sufficient to protect the equipment from access by unauthorized personnel.

b. All multiplexers will be located within a controlled access area of the sites or facilities.

c. If the multiplexers cannot be installed in the patch and test facility, they will be mounted in a cabinet with locking front and rear access panels. The ISSO or designated authority will control the key.

d. All multiplexers designed for rack mounting in equipment racks or cabinets will be mounted and properly grounded.

e. Any phone company lines used for support or maintenance on this equipment will be deactivated when not in use.

f. All vendor-supplied passwords that are required to enter the multiplexer will be changed immediately upon installation.

g. Remote configuration in all multiplexers will be disabled unless authorized by the ISSO.

6.7 NETWORK MANAGEMENT

6.7.1 Network Management Security Implications

It is MHS policy that ISSOs or NSOs will institute the following procedures:

a. Most systems default to a community name of **public**. The community name will be changed to something that is not easily guessed. It will be protected in the same way as any password is protected.

b. IP Sec will be used to secure traffic sent between network management center workstations and routers on their respective networks where possible.

c. Upgrade to SNMP (latest version) as soon as possible and feasible. Newly updated versions offer many enhanced features, such as encryption and authentication.

d. TRAP authentication will be turned off at the routers. This will aid in preventing intruders from using trap messages to discover community strings.

e. The privileged/non-privileged modes of devices that allow such services will be used, especially routers. Different community names will be used for **read-only** access and **read** and **write** access.

f. A list of specific IP addresses that are allowed to send messages to the device infrastructure will be specified.

g. Alarms will be set up within the managed network's framework. At a minimum, these include the following:

   1) **Integrity Violation:** Indicates that network contents or objects have been illegally modified, deleted, or added.

2) **Operational Violation:** Indicates that a desired object or service could not be used.

3) **Physical Violation:** Indicates that a physical part of the network (such as a cable) has been damaged or modified without authorization.

4) **Security Mechanism Violation:** Indicates that the network's security system has been compromised or breached.

5) **Time Domain Violation:** Indicates that an event has happened outside its allowed or typical time slot.

h. Notification authorities will be determined at the local AIS/network level.

i. Alarms will be categorized by severity using the following guidelines:

1) Critical and major alarms are given when a condition that affects service has arisen. For a critical alarm, steps must be taken immediately in order to restore the service that has been lost completely.

2) A **major** alarm indicates that steps must be taken as soon as possible because the affected service has degraded drastically and is in danger of being lost completely.

3) A **minor** alarm indicates a problem that does not yet affect service, but may do so if the problem is not corrected.

4) A **warning** alarm is used to signal a potential problem that may affect service.

5) An **indeterminate** alarm is one that requires human intervention to decide its severity.

j. Protocol Analyzers or sniffers are tools used to maintain a healthy computer network or to fix a problematic one. Protocol analyzers capture and interrogate individual protocol packets. All information sent in clear text, such as passwords and sensitive information, can be captured and viewed by protocol analyzers. Access to these tools will be limited and their use tightly controlled.

6.7.2 Network Management Station

At the apex of the network management structure is the management station. This device is usually a high-end workstation, most likely a Sun Scalable Processor Architecture (SPARC) or a Reduced Instruction Set Computer (RISC) platform. Applications such as HP OpenView, and Cisco Works provide the user interface to the various levels of network management mentioned above. All facets of the management umbrella are controlled from here. It is extremely important that this workstation be protected.

It is MHS policy that:

a. The management workstation will be located in a secure environment with only limited access.

b. Only those accounts necessary for the operation of the system and for access logging will be maintained.

c. A record will be maintained of all logons and transactions processed by the management station. Include time logged in and out, devices that were accessed and modified, and other activities performed.

d. Access to Network Management Stations will be restricted to known authorized users with appropriate User-IDs and passwords. Encryption should be used for passwords and entire network management sessions (e.g., system encryption or Secure Shell [SSH] client).

6.8 PACKET FILTERING AND MONITORING

Packet filtering and monitoring are essential parts of a modern network architecture. These functions have become especially important for sites with the transition from dedicated leased lines to common user communications media such as the NIPRNet. Common user communications provide economical and performance benefits. However, these benefits do present exposure to new threats, such as communications traffic interception, modification, and insertion. Two of the most important forms of protection against unauthorized use of common user communications networks are packet filtering and monitoring.

6.8.1 Site Network Connectivity Architecture

The MHS Enclave Security Architecture defines an integrated system supporting DiD. An enclave includes the **Enclave Perimeter** and **Computing Environment** layers in the DiD architecture. Enclaves may be broken down into **Security Domains** or **Communities of Interest** (COIs). A large, complex site (such as the Defense Enterprise Computing Center – Detachment [DECC-D]) may have multiple security domains with protection mechanisms tailored to the security requirements of specific customers. For example, the Defense Finance and Accounting Service (DFAS) and the Defense Logistics Agency (DLA) may have functionally driven security domains. There might also be technology-driven security domains for Multiple Virtual Storage (MVS), Unisys, Tandem, etc. Smaller locations may have a single enclave with a single security domain supporting the entire organization. A security domain would require a firewall system at a LAN-to-LAN interface, in addition to the firewall separating the LANs from the WAN at the enclave perimeter.

It is MHS policy that:

a. The ISSO/NSO will ensure that all AIS and networks under their purview use the common Enclave Security Architecture.

b. As directed by the Enclave Security Architecture, a Dual-Homed with Screened Subnet Demilitarized Zone (DMZ) architecture will be established by organizations to host their publicly accessible systems (e.g., EC/EDI, public Web servers, mail servers, external Domain Name Service (DNS), X.500 directories, etc.) within the DMZ.

c. Direct network connections between Tri-Service and TMA managed networks and the Internet, NIPRNet, Secret Internet Protocol Router network (SIPRNet), or other external networks are **not** permitted. Connections that bypass or circumvent an MHS managed firewall will be prohibited, except where reviewed and approved by the DAA and the CIO.

d. Connections over SSH and Secure Sockets Layer (SSL)-enabled applications allow users to encrypt their sessions. Such encrypted sessions will be proxied at the firewall and will not be used to bypass or circumvent Tri-Service and TMA managed firewalls.

6.8.2 Enclave Perimeter Security Mechanisms

Enclave Perimeter Security mechanisms are employed at the boundary between a MHS private LAN and a WAN (e.g., NIPRNet). Current technology limits the ability to implement Enclave Security on Asynchronous Transfer Mode (ATM) networks. Therefore, direct ATM connections between an enclave and WANs are not authorized.

6.8.2.1 Enclave Perimeter Network Intrusion Detection System (IDS)

The Network IDS is the first layer of defense in the DiD architecture. This network-based IDS capability will detect, analyze, and collect intrusive behavior occurring on networks using IP. The Network IDS is passive, so intruders are not aware of its presence. Data can be analyzed real-time or collected for retrospective analysis. Alarms are generated based on event rules.

It is MHS policy that:

a. Each Tri-Service and TMA location will install and maintain a Network IDS at its Enclave Perimeter.

b. Whenever possible, the Enclave Perimeter IDS will be positioned outside of any local firewalls so that the IDS managers have visibility of all attempted malicious activity.

The MHS TIMPO office is responsible for the review, and approval of requirements and installation for Enclave Perimeter Network IDS.

6.8.2.2 Router Access Controls Lists (ACLs)

A Router ACL provides a basic level of access control over network connections based on the site's local security guidance. These controls include restrictions on incoming and outgoing connections, as well as on connections between LAN segments internal to the site/enclave. These restrictions are based on the source and destination addresses of the IP packet as well as the service type (e.g., Simple Mail Transfer Protocol [SMTP], e-mail, Telnet, HTTP).

It is MHS policy that:

a. NSO/ISSO will implement router ACLs based on a policy of **Deny by Default** with blocks on all services and protocols not required by the site. Services and protocols with known vulnerabilities will be allowed only to required source and destination IP addresses.

b. Egress filtering rules will be applied denying all outbound traffic with illegitimate (i.e., not local network) IP addresses. This is to prevent MHS enclaves from being part of a Distributed Denial of Service (DDoS) attack. The IA Program Office will address any exceptions to requirement.

6.8.2.3 Local Enclave LAN IDS

It is MHS policy that:

a. TIMPO has the capability to provide advice, assistance, and training for IDS that are, or will be installed at MHS facilities.

b. Sites can install an IDS monitoring station and may request TIMPO assistance to customize the application for any local requirements.

c. The IDS will be configured to monitor network traffic and provide real-time alarms for network based attacks.

d. Significant incidents will be reported in accordance with MHS policy on incident reporting.

6.8.2.4 Enclave Firewall

It is MHS policy that:

a. All Tri-Service and TMA networks will use either network-layer or application-level firewalls (or gateways) to secure connections to WANs. TIMPO can provide advice and assistance with planning and installation.

b. Enclave Firewalls will be configured with the most restrictive security rules possible ("that which is not expressly allowed is denied").

c. Application-level firewalls procured for Tri-Service and TMA AISs will, at a minimum, include proxies for the following network applications:

1) Simple Mail Transfer Protocol (SMTP)

2) Hyper Text Transport Protocol (HTTP)

3) http - over Secure Sockets Layer ([SSL] HTTPS)

4) Network News Transfer Protocol (NNTP)

5) Telnet

6) File Transfer Protocol (FTP)

7) Secure Shell (SSH)

d. ISSOs and NSOs are responsible for the monitoring, auditing, and management of the enclave firewall.

6.8.2.5 Demilitarized Zone (DMZ)

It is MHS policy that:

a. A DMZ will be established within the *Enclave Security Architecture* to host any publicly accessible systems (e.g., EC/EDI, public Web servers, mail servers, external DNS, X.500 directories, etc.). The approved architecture is to build the DMZ on a separate branch (network interface) of the Enclave Perimeter firewall as part of the Screened Subnet architecture.

b. All DMZ traffic will be routed through the firewall and the DMZ will be kept separate from the rest of the network.

   Note: This method could cause load problems on the firewall if a critical amount of traffic is passing between the outside and the DMZ. If this is the case, the load issue could affect non-DMZ traffic between the protected network and the outside. Multiple firewalls or load balancing could mitigate this situation if it is predicted to be a problem.

6.8.3 Perimeter Router Filtering

The Perimeter Router is the point of entry to a site for all packets or IP datagrams from the NIPRNet and private IP circuits. Due to this position, it is the first place where packet filtering or monitoring can be performed under the control of the site. The device in general use at sites for this purpose is a Cisco 7500 series router. This device has the capability of performing packet filtering using fairly basic filtering rules. Perimeter Router filtering rules should operate at a fairly coarse level of granularity and leave the finer levels of resolution to the inner firewalls, where the throughput demands are much lower and finer levels of granularity are feasible. The IOS version running on the Perimeter Router must be 11.1 or later.

Site perimeter filtering policy is based on the principle of **Deny by Default** with blocks on all services and protocols not required by the site. The criteria for restricting or denying a service will be based on guidance from DoD-CERT bulletins, vendor security advisories, and the results of intrusion investigations.

6.8.3.1 Perimeter Router Filtering Guidance

The filtering guidelines are drawn from a variety of sources, including the CERT Advisory 10-97 (ftp://info.cert.org/pub/tech_tips/packet_filtering). The filtering guidelines can be applied to any firewall device, but at a minimum, they are to be implemented at Perimeter Routers to the fullest extent possible. Ports and services will be controlled by IP if they cannot be blocked completely for operational reasons. All non-required or unused ports and services should be blocked.

a. For diagnostics purposes ONLY, ping and trace route must be opened. Upon completion of diagnostics the ports will return to being denied.

b. NSO/ISSO will implement the following filtering guidance:

   1) Will block X Windows (TCP/User Datagram Protocol[UDP], ports 6000+) except for sites that have implemented Composite Health Care System (CHCS) II. These sites will allow ports 6000 and 6001 (e.g., command "access-list 101 deny tcp any any range 6000 6010").

6.8.3.2 Packet Filtering Policy

In Software Release 11.1, Cisco introduced the ability to assign input access lists to an interface. This allows a Network Administrator to filter packets before they enter the router instead of as they leave the router. Input access lists can be used to prevent some types of IP address spoofing, whereas output access lists alone will not provide sufficient security.

For background information on anti-spoofing, refer to the Cisco Internet Security Advisories regarding smurfing attacks, TCP SYN attacks, and Cisco's response to CERT Advisory 95-01 at http://www.cisco.com/warp/public/707/advisory.html.

6.9 FIREWALLS

Packet Filtering can be applied to any internal firewall device or router and should be implemented to the fullest extent possible. This is necessary in order to minimize the internal threat and protect the enclaves. Ports and services will be controlled by IP if they cannot be blocked completely for operational reasons. Internal firewalls or filtering rules should be based on applications being used within internal enclaves. Just as at the network perimeter, all non-required ports and services should be blocked to the most restrictive rules possible ("that which is not expressly allowed is denied").

It is MHS policy that:

a. Direct network connections between Tri-Service or TMA managed networks and the Internet, NIPRNet, or other external networks are **not** permitted.

b. All Tri-Service and TMA networks will use network-layer or application-level firewalls (or gateways) to secure connections to WANs.

c. Application-level firewalls procured for Tri-Service and TMA AIS will, at a minimum, include proxies for the following network applications:

   1) Simple Mail Transfer Protocol (SMTP)

   2) Hyper Text Transport Protocol (HTTP)

   3) http - Over Secure Sockets Layer ([SSL] HTTPS)

4) Network News Transfer Protocol (NNTP)

5) Telnet

6) File Transfer Protocol (FTP)

7) Secure Shell (SSH)

d. Connections that bypass or circumvent a Tri-Service or TMA managed firewall will be prohibited, except where reviewed and approved by the DAA.

e. Enabled applications (e.g., connections over SSH and SHL) will be proxied at the firewall and will not be used to bypass or circumvent Tri-Service or TMA managed firewalls.

f. Firewalls will be physically protected against unauthorized access.

6.9.1 Firewall Penetration Testing

> *"Since penetration testing is designed to simulate an attack and use tools and techniques that may be restricted by law, Federal regulations, and organizational policy, it is imperative to get written permission for conducting penetration testing prior to starting."*
>
> NIST Special Publication 800-42, "Draft Guideline on Network Security Testing"

To verify the firewall has the ability to stop network based attacks; firewall penetration tests are necessary. The Regional Computer Emergency Response Team (RCERT) or Army Computer Emergency Response Team (ACERT) will perform firewall penetration testing after the firewall has been installed and properly configured. These tests should concentrate on three primary areas: ports; protocol or proxy services; and application services to ensure they are safe services. Other tests to be considered include performing:

a. Attacks known to be effective against earlier releases of the firewall software.

b. Source routing attacks against the firewall, to verify that the source routing and its associated problems are not vulnerabilities.

c. Port scanning attacks against every TCP/UDP port on the firewall, to verify that the ports the firewall is supposed to close are in fact closed.

d. Attacks on any proxy services trying to gain access. Proxy services shall only allow limited use and this test would verify that they could not be compromised. This test is especially useful when the AIS/network is attacked via source routing tests.

e. Tests of all send mail daemons and checks to see if mail attacks would be effective on systems beyond the firewall (after mail has been forwarded or allowed to pass).

f. Active attacks with various routing protocols, in an attempt to destroy the current routing tables or modify the routing tables for use in further attacks.

g. Bombardment of the firewall with various denial of services attacks in an attempt to shut down communications and/or crash the firewall, e.g. Internet Control Message Protocols (ICMPs) broadcast storms brought about by IP forwarding from a remote network.

6.10 JOINT INTRUSION DETECTOR (JID)

JID is the name given to the distribution package for all DoD elements. The JID is a suite of software tools that support the detection, analysis, and gathering of evidence of intrusive behavior occurring on Ethernet or Fiber Distributed Data Interface (FDDI) based networks using IP. In support of these services, JID provides four common operating models:

a. Retrospective intrusion analysis

b. Real-time intrusion detection

c. Evidence gathering

d. Statistics gathering

Many legal issues face DoD sites that perform network monitoring. Every DoD site should clarify these issues with its legal counsel before starting to monitor.

6.10.1 JID Usage

6.10.1.1 The following are guidelines on JID distribution:

a. The DoD CERT will make JID available upon request to customers who have a legitimate and demonstrated requirement for network monitoring capability.

b. Authorized customers will not further distribute JID.

c. Each DoD site will be required to ensure that their usage of JID follows the guidelines presented in this document.

6.10.1.2 The following are guidelines on JID usage:

a. Each DOD site using JID will ensure that each system being monitored at the site has DOD General Counsel and Department of Justice (DoJ) approved logon warning banners displayed to each user during each logon process.

b. With the appropriate banners in place, a network monitor will only be used to monitor activity on a system-wide level without the targeting of any specific person(s) until any suspected unauthorized activity has been identified. Once an individual has been identified as possibly being the party responsible for the suspicious activity, the appropriate Law Enforcement Agency (LEA) will be notified and will issue authorization to legally continue monitoring of the individual.

c. The DoD-CERT will be notified through the Regional CERT about any identified suspicious activity.

d. JID monitoring and data review will only be performed by trusted system administration and security personnel with a legitimate need-to-know for the information. Authorized reviewers of JID output will be identified in writing by the AIS environment's Commanding Officer.

e. Data collected as evidence to support a LEA investigation will be coordinated with the LEA performing the investigation to ensure that it conforms to accepted standards for evidence.

f. The media used to store any intended evidence will be handled in accordance with LEA policy and regulations for evidence handling.

6.10.2 JID Protection

The following are guidelines on JID administration:

a. JID source code will be stored on an off-line (i.e., not connected to any network) system or storage device.

b. Only the binary executable files of JID will be stored on the system performing the monitoring.

c. The monitoring system will be configured such that it does not allow incoming network connections from any other system, except from SSH for specifically authorized IP addresses (i.e., passively monitor the network without accepting Telnet, FTP, e-mail, etc., connections from other systems).

d. JID access will be restricted to specifically authorized personnel.

6.10.3 JID Detection Rules

JID Detection Rules are distributed by the Regional CERT, and the Regional CERT loads those rules onto the active JID systems.

6.11 Software Security

6.11.1 Operating System Software

SAs will follow DoD 8510.1-M (DITSCAP Application Manual, page 147, Appendix 2) and MHS policies and/or guidance regarding standard configurations and security requirements for operating systems. The operating system software employed to process requests by one or multiple users including AISs, controls user access to resources. The software should have the capability to identify, journal, report, and assign accountability for the operating system functions performed or attempted by a user. The software should also be able to deny user access to capabilities or resources that have not been authorized.

It is MHS policy that Operating System software must be able to:

a. Prevent a user program from executing privileged instructions.

b. Isolate the programs and data areas of one user from those of other users and the operating system software.

c. Assure error detection when directly accessing memory, accessing memory outside the programs authorized memory region, or accessing hardware registers.

d. Display a warning banner at logon to indicate that access is restricted to authorized users for legitimate work purposes only and subject to monitoring by system administrators.

e. Be maintained by the minimum number of authorized persons.

f. Should be copied after each modification and the copy immediately stored as a backup for emergency use.

6.11.2 Application Software

It is MHS policy that the following process will be followed before installing application software on an AIS/Network:

a. Define security requirements and gain security specifications approved by the group that specified the application software functional requirements, prior to acquiring or starting development of applications, or prior to making a substantial change to the existing application.

b. Conduct periodic design reviews during the developmental process to assure that the proposed design satisfies the functional and security requirements specified by the user.

c. Thoroughly test new or substantially modified sensitive applications prior to implementation to verify that the user functions and the required administrative, technical, and physical safeguards are present and are operationally adequate. This is accomplished as part of the C&A process.

d. Use simulated data and files rather than live sensitive data or files to test applications software until the software's integrity has been reasonably assured.

e. Place application software into production status after the system tests have been successfully completed and the application has been properly certified and accredited. Prototypes and pilot test versions of application software that process production data must be certified and accredited before deployment or implementation.

f. Training must be made available to application users.

g. Assign accountability for the application functions performed or attempted by a user and deny user access to capabilities or resources, which have not been authorized.

h. Maintain and protect current backup copies of critical application software, documentation, databases, and other resources required for system operation. Have backup copies readily available for use following emergencies. Assure that backup copies of the application software are in a form that can be installed on equipment described in the contingency plan.

i. The Contingency Plan must be exercised.

j. Re-certify sensitive applications every three years or following major changes.

k. Provide the same degree of protection to software documentation as provided for the software.

6.12 SECURITY PROCESS FOR WEB SITE ADMINISTRATION

This section delineates policy and assigns responsibility related to establishing, operating, and maintaining unclassified Web sites in support of the DoD MHS TRICARE healthcare program for military personnel, their families, survivors and retirees. This policy applies to MHS publicly and non-publicly accessible unclassified Web sites that are managed by the TRICARE Management Activity (TMA), to include the PEO and PMOS.

Use of the World Wide Web (WWW) has been endorsed and strongly encouraged by the DoD. The WWW is viewed as a powerful tool to convey information quickly and efficiently on a broad range of topics relating to its activities, objectives, policies and programs. As the preeminent DoD health care provider, MHS has embraced the technology of the WWW in efforts to keep its beneficiaries informed about their benefits, changes in TRICARE, downloadable forms, and a host of other conveniences.

Benefits associated with use of the WWW must be carefully balanced through the application of a comprehensive risk management program to defend against the potential risk to DoD and MHS interest, such as individual privacy, patient medical data, and national security.

It is MHS policy that:

a. Each MHS Web site will implement technical security best practices with regard to its establishment, maintenance, and administration.

b. FOR OFFICIAL USE ONLY (FOUO) or information not specifically cleared and marked as approved for public release, patient information, or information of questionable value to the general public shall not be posted to Web sites accessible to the general public. In accordance with DoD and MHS policy, patient information is considered FOUO.

c. Web sites wishing to post information referenced above must employ additional security, in accordance with the DoD's Web Site Policy and access controls, and should not be accessible to the general public.

d. The MHS CIO shall:

1) Establish a process for the identification of information appropriate for posting to Web sites, in accordance with the DoD's Web Site Policy, and ensure it is consistently applied.

2) Ensure all information placed on publicly accessible Web sites is properly reviewed for security, levels of sensitivity and other concerns before it is released. Detailed requirements for clearance of information for public release can be found in DoDD 5230.9, "Clearance of DoD Information for Public Release," and DoDI 5230.29, "Security and Policy Review of DoD Information for Public Release."

3) Ensure approved DoD security and privacy notices and applicable disclaimers are used on all Web sites under their purview.

4) Ensure all information placed on publicly accessible Web sites is appropriate for worldwide dissemination and does not place national security, DoD personnel and assets, mission effectiveness, or the privacy of individuals at an unacceptable level of risk.

5) Ensure procedures are established for management oversight and regular functional review of the Web site.

6) Ensure operational integrity and security of the computer and network supporting the Web site is maintained.

7) Ensure that reasonable efforts are made to verity the accuracy, consistency, appropriateness, and timeliness of all information placed on the Web site.

8) Ensure that a comprehensive, multi-disciplinary security assessment is conducted of Web sites within 120 days of the effective date of this document, and at least annually thereafter.

9) Ensure all Web sites are certified and accredited or reaccredited in accordance with DoDI 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)." This requirement includes Web servers currently in operation and all future Web servers.

10) Ensure security of Web sites complies with requirements mandated in the HIPAA Act.

11) Ensure all Web site administrators are trained in Web server security techniques.

12) Ensure all Web site administrators secure their Web sites by applying appropriate Web server security techniques.

13) Ensure Configuration Management, as defined in DoDI 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," is exercised to address security ramifications before new software applications or changes to the server configuration are approved.

6.13 System Acquisition Security

An Acquisition Program is a directed, funded effort designed to provide a new, improved, or continuing material, weapon, or information system or service capability in response to a validated operational or business need. DoD, in efforts to ensure IA is addressed during system development/acquisition/procurement, published DEPSECDEF Memorandum, "Defense Acquisition," October 30, 2002. In accordance with the memorandum, it is DoD policy that DoD Components shall not award a contract for the acquisition of a mission-critical or mission-essential IT system, at any level until:

a. The Component registers the system with the DoD CIO.

b. The DoD CIO determines the system has an appropriate IA strategy.

c. The Component CIO confirms that the system is being developed in accordance with the Clinger-Cohen Act (CCA) by complying with the following requirement(s):

   1) The DoD CIO will review the Component CIO's determination of CCA compliance for sufficiency before contract award for acquisition programs. For mission-critical or mission-essential IT, the IA strategy shall be submitted to the DoD CIO for review. For contracts, the DoD CIO's determination that the IA strategy is appropriate will generally be based on the certification of the Component CIO. However, even if a certification has been provided, the DoD CIO may conduct a more detailed review of such IA strategies.

The MHS IA Program Office is available to provide guidance for establishing security requirements and specifications for system/network acquisitions and ensuring that these requirements are defined in statements of work and contracts.

6.14 ENCRYPTION

There currently are no DoD requirements to encrypt SBU information; however, with the pending final HIPAA ruling, encryption of patient information may become a requirement. SBU information, e.g., personal and patient-specific information, still requires protection. Activities which currently have a need to encrypt SBU information will adhere to the encryption standards contained in FIPS Pub 46-3, "Data Encryption Standard (DES)," October 25, 1999. The DES specifies two FIPS approved cryptographic algorithms as required by FIPS PUB 140-2, "Security Requirements for Cryptographic Modules," May 25, 2001and Advanced Encryption Standard (AES), FIPS-197. When used in conjunction with ANSI X9.52 standard, FIPS PUB 46-3 provides a complete description of the mathematical algorithms for encrypting (enciphering) and decrypting (deciphering) binary coded information.

6.14.1 Virtual Private Networks (VPN)

A VPN is a distributed collection of networks or systems that are interconnected via a public network (i.e., NIPRNet or the Internet) but protect their communications through the use of encryption. In effect, a VPN is a private network distributed securely, and tunneled across a public network. Typically, VPN encryption is implemented at the local network entry point (i.e., the firewall or Premise Router), thereby freeing the end systems from having to provide the necessary encryption or communications security functions. VPN devices and software provide, not only encryption functions, but also network access control to secure Internet tunnels between remote sites.

Tunnel mode VPN encrypts entire packets, including header information, and encapsulates it within a new packet with header information reflecting only the VPN IP address and port. This is very secure since the original IP header information is encrypted. The utilization of transport mode VPNs is insufficient from a security point of view. Transport mode VPNs only encrypts the payload of a packet, leaving the header information in the clear. It is the header information that can be used to plan out an attack on a system and should be protected. Internet Key Exchange (IKE) VPN tunnels utilize tunnel mode exclusively within the MHS VPN architecture. The Secure Key Interchange Protocol (SKIP) VPN can function under both transport and tunnel modes; however, tunnel mode is utilized for the added security. A list of NIST validated COTS products for cryptographic standards can be found at: http://niap.nist.gov/niap/services/validated-products.html.

It is MHS policy that:

a. VPNs will be established as tunnel mode VPNs, which terminate outside the firewall.

b. IKE or SKIP VPN tunnels will be employed exclusively within the MHS VPN architecture.

c. The VPN architecture will be a fully meshed, centrally administered VPN. As a result, MHS "sites" (e.g. MTFs) do not retain administrative control privileges and oversight of the VPN device.

d. A VPN must provide privacy and integrity of data as it traverses the network.

e. User Authentication – The solution must verify a user's identity and restrict VPN access to authorized users. In addition, the solution must provide audit and accounting records that reflect what information was accessed, when it was accessed, and who accessed it.

f. Address Management – The solution must assign a client's address on the private net, and must ensure that private addresses are kept private.

g. Data Encryption – Data encryption will be accomplished in accordance with FIPS Pub 46-3 and FIPS Pub 140-2, "Security Requirements for Cryptographic Modules." The VPN solution must also generate and refresh encryption keys for the client and server.

6.15 DoD Key Management Infrastructure (KMI) and Public Key Infrastructure (PKI)

The DoD Key Management Infrastructure (KMI) is the critical underpinning of the Department's IA capabilities and is a vital element in achieving a secure IA posture for the Defense Information Infrastructure (DII). Accordingly, it is imperative that the Department takes an aggressive approach in acquiring a KMI that meets the requirements for all IA services. The DoD Public Key Infrastructure (PKI) is an essential element and a major component of the KMI.

6.15.1 Public Key Infrastructure

PKI is a system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances that are important in protecting sensitive communications and transactions. PKI allows the user to conduct business electronically with the confidence that (1) the person sending the transaction is actually the originator, (2) the person receiving the transaction is the intended recipient, and (3) data integrity has not been compromised.

DoD PKI refers to the framework and services that provide the generation, production, distribution, control, revocation, archive, and tracking of public key certificates and management of the public and private keys. DoD PKI provides support to applications providing the following services:

a. Confidentiality, which supports the protection of both sensitive and classified information from unauthorized disclosure.

b. Authentication, which supports verifying the identity of an individual or entity and the authority to access specific categories of information.

c. Data integrity, which supports protection of information against unauthorized modification or destruction.

d. Non-repudiation, which provides assurance to the sender of data with proof of delivery and to the recipient of the sender's identity, so that neither can later deny having processed the data.

Assistant Secretary of Defense Memorandum, "Department of Defense Public Key Infrastructure," August 12, 2000, states that the "DoD Components shall be responsible for planning, programming, and budgeting to implement the DoD PKI according to this policy, and to develop the required policy and plans to ensure a standard implementation of the DoD PKI within their respective organizations; coordinate with the DoD PKI Program Management Office (PMO) and Defense-wide Information Assurance Program (DIAP) in these duties as required; immediately transition from use of any non-DoD PKI to the DoD PKI."

Appendix F, *MHS Public Key Infrastructure (PKI)/Public Key Enabling (PKE) Guidance* has been developed to aid the MHS in obtaining the necessary DoD PKI/PKE objectives.

6.16 COMPUTER VIRUSES

Computer viruses are programs written to cause intentional damage to AISs and networks. These programs have the ability to replicate themselves to other computers or programs. Defense against viruses is difficult because of this particularly dangerous ability to replicate.

6.16.1 Virus Activity

AIS and network developers must take precautions to prevent viruses from infecting an AIS. At least one copy of virus free source and executable code should be archived. All source or executable code should be protected by checksum or another safeguard to ensure that approved code is not altered. When an AIS and network is installed, verify the checksum or other safeguard.

6.16.2 Computer Virus

Recent incidents of computer viruses within DoD and elsewhere indicate the need to use prudent practices to prevent the introduction and proliferation of malicious software in the workplace. All software to be loaded on a system must first be scanned for viruses. All users of Tri-Service and TMA AISs and networks are to report suspected virus activity observed to their local supervisor or ISSO.

a. Suspicious activity includes:

   1) Suspected or unauthorized misuse of government resources.

   2) Use of an AIS and network or AIS and network account by another party.

   3) Illegal copying of software.

   4) Abnormal activity on an AIS, which may indicate the presence of a computer virus.

b. Some of the ways in which viruses are propagated include:

   1) Sharing infected diskettes between users.

   2) Downloading programs from public electronic bulletin boards.

3) Passing virus laden e-mail attachments.

4) Passing infected demonstration or system diskettes.

6.16.3 Main Virus Indicators

The main indications of viruses are changes in file sizes and contents, the unexplained appearance of unknown files or the reassignment of system resources (see **Figure 7**). The unaccounted uses of RAM or reductions in the amount of RAM known to be in the machine are important indicators. Some viruses have indicators written into their programs, such as messages, music, and graphical displays.

VIRUS INDICATORS
• Warning message from anti-viral software.
• Strange messages or graphics.
• Drive lights blinking.
• Missing files and/or data.
• Running out of memory.
• Increased file size.
• Program taking longer to load than normal.

Figure 7. Virus Indicators

6.16.4 Virus Prevention

Anti-virus practices and techniques described below should be employed by all MHS AIS and network users (see **Figure 8**). These practices minimize the risk of introducing viruses and other malicious software, ensure timely detection of viral infections, eliminate viral infections from the inventory of microcomputers, and minimize the risk from malicious programs to larger AISs or network systems.

There are documented instances in which commercial “shrink wrapped” software was inadvertently distributed containing viruses. Check all new software for infection before running it for the first time. It is even advisable to use different anti-virus programs, since no single virus scanner is able to detect all viruses.

Only approved software will be installed on workstations unless the ISSO has authorized the software for use and scanned it for viruses. Public domain software, shareware, freeware, computer games, software copied from a home system, downloaded from the Internet, or another user’s system are frequent sources of viruses and should not be installed on any Tri-Service or TMA system without authorization from the ISSO.

It is recommended that users do not download software from public Web sites. Public Web sites are a source of computer viruses. When it is necessary, download to a diskette when downloading from an authorized source and use virus scanning software to test for viruses before copying files to a hard disk. Software should not be download to a network server.

VIRUS PREVENTION

- Scan new software.
- Use only authorized software.
- Do not download software from public bulletin boards.
- Do not copy and share software.
- Scan diskettes from home and external sources.
- Make backups of critical files.
- Beware of shareware and freeware.
- System Administrators will install, maintain, and update anti-virus software on all servers and workstations.
- System Administrators will ensure the Server Anti-Virus' "Automatic Scan" feature is turned on at all times for all network servers.

Figure 8. Virus Prevention

Do not use diskettes from home systems or other external sources that have not been approved and scanned for viruses. These diskettes may be infected. Do not copy copyrighted software or share software with other employees. Copying and sharing software are common ways of spreading computer viruses in a personal computer environment in addition to potentially violating copyright laws.

Backup copies of protected system files, critical data files and applications (backup copies of applications for archival purposes generally do not represent a copyright violation) and store them on write protected diskettes. A network administrator should have a backup copy of every software program every time it is modified in accordance with established software development procedures and controls. This provides some assurance that a clean backup exists in the event a virus hits. The administrators should also periodically scan the servers for viruses.

6.16.5 Virus Response

If a computer is believed to be infected with a virus, then the steps listed in **Figure 9** should be followed. Some attempts to remove a virus will do much more damage than the virus itself could have done. Viruses can be extremely unforgiving unless they are removed correctly.

RESPONSE TO SUSPECTED VIRUS	
Stop	Do not turn off the PC
Take Notes	Identify what activity indicated a virus may be present
Get help	Contact your Supervisor, ISSO, or Help Desk

Figure 9. Response to Suspected Virus

Report all suspicious activity to your supervisor, ISSO, or help desk. The suspicious activity may be caused by something other than a virus. If it is a virus, only a rapid response will result in its successful containment and removal. Once determined that it is a virus, the need exists to eradicate the virus, prevent its spread and re-infection, and bring the newly cleaned system back into full production.

6.17 MOBILE CODE

Mobile code is a powerful software tool that enhances cross-platform capabilities, the sharing of resources, and Web-based solutions among networks. Its use is widespread and increasing in both commercial and government applications and may be employed in systems supporting functional areas ranging from acquisition to intelligence to transportation.

Mobile code has the potential to severely degrade operations if improperly used or controlled. It may affect the confidentiality, availability, or integrity of operations by such means as transparently altering or exporting data, files, inserting backdoors into networks, or permitting remote control of client systems, capturing keystrokes or data packets, or permitting distributed denial of service attacks to emanate from compromised systems. The security measures prescribed by DoD Memorandum, “Policy Guidance for Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems,” dated 7 November 2000, is considered the basis for the categories, risk assessments, and ratings assigned to various mobile code technologies from trusted sources that may be employed by the MHS.

It is MHS policy that:

a. CIOs, PEO, PMs, Executive Agents (EAs), and ISSOs be familiar with mobile code technologies and the DoD documents that establish rules relating to mobile codes.

b. PEO, PMs, EAs, and ISSOs develop a mobile code risk mitigation strategy as part of the risk management plan required in DoDI 5200.40, “Defense Information Technology Security Certification and Accreditation Process (DITSCAP).” The strategy must be attached to each system’s accreditation package as part of the SSAA.

c. Whenever possible, the automatic execution of all categories of mobile code in e-mail be disabled and desktop software be configured to prompt the user prior to opening attachments that may contain mobile code.

6.18 WIRELESS COMMUNICATIONS

Wireless technology permits the transfer of information (active or passive) between separated points without physical connection. Currently, wireless technologies use infrared (IR) and radio frequency (RF) and optical wireless (a.k.a. "Free Space Optics") but, as technology evolves, wireless could include other methods of transmission. Active information transfer entails emanation of energy, whereas passive information transfer includes stand-alone storage devices that can record audio and video information.

Appendix D of this Manual, *Wireless Devices Policy*, outlines policy and procedures for wireless services, devices, and technological implementations for TMA and MHS Tri-Service AISs and networks.

Appendices

Appendix A - References

The following listing of Federal Laws, Bulletins, and DoD Regulations and Directives provides a reference source of documents pertaining to automated information systems processing sensitive unclassified and classified information. They are organized in the following hierarchy:

- Federal Laws
- Federal Guidelines (Guidelines/Bulletins/Publications/Executive Orders)
- Department of Defense Directives
- Department of Defense Instructions
- Department of Defense Manuals
- Department of Defense Regulations
- Memorandums
- Other References

Federal Laws

- Privacy Act of 1974 (Public Law 93-579).
- Computer Fraud and Abuse Act of 1984 (Public Law 98-473).
- Computer Fraud and Abuse Act of 1986 (Public Law 99-474).
- Freedom of Information Act of 1986 (Public Law 99-570).
- Computer Security Act of 1987 (Public Law 100-235).
- Computer Matching and Privacy Protection Act of 1988 (Public Law 100-503).
- Health Insurance Portability and Accountability Act of 1996 (Kennedy-Kassebaum/HIPAA), (Public Law 104-191) August 21, 1996, December 28, 2000.

Federal Guidelines

- Department of Defense Password Management Guideline, April 12, 1985.
- Federal Information Processing Standards Publication (FIPS Pub) 31, “Guidelines for Automatic Data Processing Physical Security and Risk Management,” June 1974. (Federal Register notice dated November 13, 1998 on the proposed withdrawal of FIPS PUB 31).

- Federal Information Processing Standards Publication (FIPS Pub) 73, "Guidelines for Security of Computer Applications," June 30, 1980.

- Federal Information Processing Standards Publication (FIPS Pub) 112, "Password Usage," May 30, 1985.

- Federal Information Processing Standards Publication (FIPS Pub) 140-2, "Security Requirements for Cryptographic Modules," May 25, 2001.

- Federal Information Resources Management Regulation (FIRMR) Bulletin C-22, "Security and Privacy Protection of Federal Information Processing (FIP) Resources."

- Federal Information Resources Management Regulation (FIRMR), Title 41, Code of Federal Regulations, Chapter 201.

- OMB Bulletin, "The Conduct of Matching Programs," April 13, 1989.

- OMB Circular No. A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Systems," November 30, 2000.

- OMB Memorandum M-99-18, "Privacy Policies of Federal Web Sites," June 2, 1999.

- Presidential Decision Directive 63, "Critical Infrastructure Protection," May 22, 1998.

Department of Defense Directives

- DoDD 5136.12, "TRICARE Management Activity (TMA)," May 31, 2001.

- DoDD 5200.1, "DoD Information Security Program," December 13, 1996.

- DoDD 5200.8, "Security of DoD Installations and Resources," April 25, 1991.

- DoDD 5230.9, "Clearance of DoD Information for Public Release," April 9, 1996. (Change 1, July 15, 1999, WHS.)

- DoDD 6000.12, "Health Services Operations and Readiness," April 29, 1996. (Change 1, January 20, 1998 ASD (HA).)

- DoDD 8000.1, "Management of DoD Information Resources and Information Technology," February 27, 2002. (Change 1, March 20, 2002 ASD (C3I).)

- DoDD 8500.1, "Information Assurance (IA)," October 24, 2002.

- DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997.

- DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 6, 1999.

Department of Defense Manuals

- DoD 8510-M, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July 31, 2000.

Department of Defense Regulations

- DoD 5200.2-R, "Personnel Security Program," January 1987.
- DoD 5400.11-R, "Department of Defense Privacy Program," August 31, 1983.
- DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998.

Memorandums

- Assistant Secretary of Defense Memorandum, "Department of Defense (DoD) Public Key Infrastructure," August 12, 2000.
- Assistant Secretary of Defense Memorandum, "Policy Guidance for use of Mobile Code Technologies in Department of Defense (DoD) Information Systems," November 7, 2000.
- Chairman, Joint Chiefs of Staff Memorandum, 6211.02A, "Defense Information System Network and Connected Systems, May 22, 1996.
- Deputy Secretary of Defense Memorandum, "Defense Acquisition," October 30, 2002.
- Deputy Secretary of Defense Memorandum, "Department of Defense (DoD) Information Assurance Vulnerability Alert (IAVA)," December 30, 1999.
- Deputy Secretary of Defense Memorandum, "Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 4-8460 – Department of Defense Global Information Grid Networks," August 24, 2000.
- Deputy Secretary of Defense Memorandum, "Department of Defense Public Key Infrastructure," May 6, 1999.
- Deputy Secretary of Defense Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," May 29, 2001.
- Deputy Secretary of Defense Memorandum, "Smart Card Adoption and Implementation," November 10, 1999.
- Office of the Assistant Secretary of Defense (DA&M) Memorandum, "Privacy Act Computer Matching Programs," July 19, 1989.
- Office of the Secretary of Defense Memorandum, "Common Access Card," January 16, 2001.

- Office of the Secretary of Defense Memorandum, “Increasing the Security Posture of the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet), August 22, 1999.

- Office of the Secretary of Defense Memorandum, “Privacy Policies and Data Collection on DoD Public Web Sites,” July 13, 2000.

- “X.509 Certificate Policy for the United States Department of Defense,” Version 5.2, November 13, 2000.

Other References

- DISA Network Infrastructure Security Technical Implementation Guide (STIG), V3, R1, December 8, 2000.

- DISA Web Application Security Technical Implementation Guide (STIG), V2, R1, March 31, 2000.

- DoD Web Site Administration Policies and Procedures, November 25, 1998.

- “Public Key Infrastructure Roadmap for the Department of Defense,” Version 5.0 December 18, 2000.

- National Computer Security Center, NCSC-TG-004 (Aqua Book), “Glossary of Computer Security,” Version 1, October 21, 1988.

- National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, National information systems Security (INFOSEC) Glossary, September 2000.

Appendix B - Definitions

Access – A specific type of interaction between a subject and an object resulting in the flow of information from one to the other.

Access Control – The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network).

Access Control Mechanism – Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access in an automated system.

Access Level – The hierarchical portion of the security level used to identify the sensitivity of data and the clearance or authorization of users. Note: The access level, in conjunction with the non-hierarchical categories, forms the sensitivity label of an object.

Access Types – The nature of an access right to a particular device, program, or file (e.g., read, write, execute, append, modify, delete, or create).

Accountability – The property that enables activities on a system to be traced to individuals who may then be held responsible for their actions.

Accreditation – A formal declaration by the DAA that the AIS and network is to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of AISs and networks on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

Assurance – A measure of confidence that the security features and architecture of an AIS and network accurately mediate and enforce the security policy.

Audit Trail – A chronological record of system activities sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.

Authenticate – To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

Authorization – The granting of access rights to a user, program, or process by a responsible administrator.

Automated Information System – An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

Automated Information Systems Security – Measures and controls that protect an AIS and network against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data. AIS and network security includes consideration of all hardware and/or software functions.

Availability of Data – Timely reliable access to information and information services for authorized users.

Backup – A copy of data and/or applications contained in the AIS/network stored on magnetic media outside of the AIS/network to be used in the event AIS/network data are lost.

Certification – The comprehensive evaluation of the technical and non-technical security features of an AIS/network and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

Compromise – A violation of the security policy of a system such that unauthorized disclosure of sensitive information may have occurred.

Computer Fraud – Computer-related crimes involving deliberate misrepresentation, alteration or disclosures of data in order to obtain something of value (usually for monetary gain). A computer system must have been involved in the perpetration or cover-up of the act or series of acts. A computer system might have been involved through improper manipulation of input data; output or results; applications programs; data files; computer operations; communications; or computer hardware, systems software, or firmware.

Computer Matching Program – Any computerized comparison of two or more automated systems of records or a system of records with non-Federal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or for recouping payments or delinquent debts under Federal benefit programs. Further, matching programs include any computerized comparison of automated Federal personnel two or more or payroll system of records, or a system of Federal personnel or payroll records with non-Federal records.

Confidentiality – Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Configuration Control – The process of controlling modifications to the system's hardware, firmware, software, documentation, test, test fixtures, and test documentation that provides sufficient assurance that the system is protected against the introduction of improper modifications prior to, during, and after system implementation. See configuration management.

Configuration Management – The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, test, test fixtures and test documentation throughout the development and operational life of the system. See configuration control.

Contingency Plan – A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

Controlled Access Protection – Access control through login procedures, audit of security relevant events, and resource isolation.

Countermeasure – Any action, device, procedure, technique, or other measure that reduces the vulnerability of or threat to a system.

Criticality – Any information or applications, which are so important to the organization that little or no loss of availability is acceptable.

Cryptography – The principles, means and methods for rendering information unintelligible and for restoring encrypted information to intelligible form.

Data – A representation of facts, concepts, information or instructions suitable for communication, interpretation, or processing by users or by an AIS.

Data Encryption Standard – A cryptographic algorithm for the protection of unclassified data, published in Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology, is intended for public and government use.

Data Integrity – The state that exists when automated data is the same as that in source documents, or has been correctly computed from source data, and has not been exposed to alteration or destruction.

Defense-in-Depth – The security approach whereby layers of IA solutions are used to establish an adequate IA posture. Implementation of this strategy also recognizes that due to the highly interactive nature of the various systems and networks, IA solutions must be considered within the context of the shared risk environment and that any single system cannot be adequately secured unless all interconnected systems are adequately secured.

Degauss – To demagnetize a tape or other magnetic storage media leaving little or no magnetically stored information.

Denial of Service – Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service.

Designated Approving Authority – The official who has the authority to decide on accepting the security safeguards prescribed for an AIS and network or that official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards.

Disaster Recovery Plan – A plan for emergency response, backup operations, and post-disaster recovery to ensure the availability of critical resources and continuity of operations in an emergency.

Discretionary Access Control – A means of restricting access to objects based on the identity and need-to-know of the user, process and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Encryption – A procedure to convert plain text into cipher text.

External Certificate Authority – An agent that is trusted and authorized to create, sign and issue certificates to approved vendors and contractors for the purpose of enabling secure interoperability with DoD entities.

Identification – The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.

Information Assurance – Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Information Systems Security Officer – The person responsible for ensuring that security is provided for and implemented throughout the life-cycle of an AIS/network from the beginning of the concept development plan through its design, development, operation, maintenance, and secure disposal.

Information Assurance Vulnerability Alert – Comprehensive distribution process for notification of CINCs, Services and Agencies about vulnerability alerts and countermeasures information.

Integrity – Quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the information structures and occurrence of the stored information. It is composed of data integrity and system integrity.

Interim Approval to Operate – Temporary authorization granted by a DAA for an IS to process information based on preliminary results of a security evaluation of the system.

Isolation – The containment of subjects and objects in a system in such a way that they are separated from one another, as well as from the protection controls of the operating system.

Least Privilege – The principle that requires each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Mission Critical – Systems handling information, which is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.

National Computer Security Center – Originally named the DoD Computer Security Center, the NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the Federal Government.

Need-To-Know – The necessity for access to, knowledge of, or possession of specific information required to carry out official duties.

Network – A network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information.

Non-repudiation – The method by which the sender of information is provided with proof of delivery and the recipient is assured of the sender's identity so that neither can later deny having processed the information

Object – A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, and network nodes.

Object Reuse – The reassignment and reuse of a storage medium (e.g., page frame, disk sector, and magnetic tape) that once contained one or more objects. To be securely reused and assigned to a new subject, storage media must contain no residual data (magnetic remnants) from the object(s) previously contained in the media.

Operational Testing – The segment of security testing in which the advertised security mechanisms of the system are tested, under operational conditions, for correct operation.

Password – A protected, private character string used to authenticate an identity.

Penetration Testing – The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The evaluator's work under the same constraints applied to ordinary users.

Permissions – A description of the type of authorized interactions a subject can have with an object. Examples include read, write, execute, add, modify, and delete.

Personal Digital Assistant – A hand-held computer that helps with such tasks as taking notes, scheduling appointments, and sending faxes and electronic mail. PDAs are also called Personal Communicators and Personal Intelligent Communicators.

Personal Information – Information about an individual that is intimate or private to the individual, as distinguished from information related solely to the individual's official functions or public life.

Personnel Security – The procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances.

Physical Security – The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.

Privileges – A set of authorization/permissions granted by an authorized officer to an AIS and network or network user to perform certain operations.

Public Key Infrastructure – An enterprise-wide service that supports digital signatures and other public key-based security mechanisms for DoD functional domain programs, including generation, production, distribution, control and accounting of public key certificates.

Reliability – The quality of producing the same results each time the same procedures and products are used, usually implying dependable equipment and bug-free processing routines.

Residual Risks – The portion of risk that remains after security measures have been applied.

Risk – The probability that a particular threat will exploit a particular vulnerability of the system.

Risk Analysis – The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management.

Risk Assessment – An assessment of a system based on the sensitivity of information processed, or to be processed, and the clearances of users to determine the Security Class of the system.

Risk Management – The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and testing, security evaluation of safeguards, and overall security review.

Safeguards – An implementation of technology or techniques to protect confidentiality, integrity, and availability.

Security Evaluation – An evaluation done to assess the degree of trust that can be placed in systems for the secure handling of sensitive information. One type, a product evaluation, is an evaluation performed on the hardware and software features and assurances of a computer product from a perspective that excludes the application environment. The other type, a system evaluation, is done to access a system's security safeguards with respect to a specific operational mission and is a major step in the C&A process.

Security Features – The security-relevant functions, mechanisms, and characteristics of system hardware and software. Security features are a subset of system security safeguards.

Security Measures – Elements of software, firmware, hardware, or procedures included in a system for the satisfaction of security specifications.

Security Policy – The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Requirements – The types and levels of protection necessary for equipment, data, information, applications, personnel and facilities to meet security policy.

Security Requirements Baseline – A description of minimum requirements necessary for a system to maintain an acceptable level of security.

Security Safeguards – The protective measures and controls prescribed to meet the security requirements specified for a system. Those safeguards may include but are not necessarily limited to: hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices.

Security Specifications – A detailed description of the safeguards required to protect a system.

Security Test and Evaluation – An examination and analysis of the security safeguards of a system as they have been applied in an operational environment to determine the security posture of the system.

Sensitive But Unclassified – Information, the disclosure, loss, misuse, alteration or destruction of which could adversely affect national security or other Federal Government interests.

Sensitive Information – Any information, the loss, misuse, modification of, or unauthorized access to, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, (The Privacy Act) but has not been specifically authorized under criteria established by an Executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

System Availability – The state that exists when required automated information services can be performed within an acceptable time even under adverse circumstances.

System Integrity – The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Technical Vulnerability – A hardware, firmware, communication, or software flaw that leaves a computer processing system open for potential exploitation, either externally or internally, thereby resulting in risk for the owner, user, or manager of the system.

Terminal Identification – The means used to uniquely identify a terminal to a system.

Threat – Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.

Threat Agent – A method used to exploit a vulnerability in a system, operation, or facility.

Threat Analysis – The examination of all actions and events that might adversely affect a system or operation.

Threat Monitoring – The analysis, assessment, and review of audit trails and other data collected for the purpose of searching out system events that may constitute violations or attempted violations of system security.

Trusted Computer System – A system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information.

Trusted Computing Base – The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to enforce correctly a unified security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user’s clearance level) related to the security policy.

User – Person or process accessing an AIS or network either by direct connections (i.e., via terminals), or indirect connections (i.e., prepare input data or receive output not reviewed for content or classification by a responsible individual).

User ID – A unique symbol or character strings used by a system to identify a specific user.

Virus – A self-propagating computer program composed of a mission component, a trigger component, and a self-propagating component.

Vulnerability – A weakness in system security procedures, system design, implementation, internal controls, etc. that could be exploited to violate system security policy.

Appendix C - Acronyms

ACERT	Army Computer Emergency Response Team
ACL	Access Control List
ADP	Automated Data Processing
AES	Advanced Encryption System
AIS	Automated Information System
ANI	Automatic Number Indicator
ANSI	American National Standards Institute
AP	Access Point
APG	Automatic Password Generator
ASD	Assistant Secretary of Defense
ATM	Asynchronous Transfer Mode
ATO	Approval to Operate
BI	Background Investigation
C&A	Certification and Accreditation
CA	Certification Authority
CAC	Common Access Card
CAP	Connection Approval Process
CAPP	Controlled Access Protection Profile
CBT	Computer Based Training
CCA	Clinger-Cohen Act
CCB	Configuration Control Board
CCSD	Commercial Circuit System Designators
CD	Carrier Detect -or- Compact Disk
CERT	Computer Emergency Response Team
CHCS	Composite Health Care System
CINC	Commander In Chief
CIO	Chief Information Officer
CND	Computer Network Defense
COCO	Contractor Owned, Contractor Operated
COI	Community of Interest
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan

COTR	Contracting Officer's Technical Representative
COTS	Commercial Off-The-Shelf
CPS	Certificate Practice Statement
CSC	Computer Security Center
CSEC	Computer System Evaluation Criteria
CSMA/CD	Carrier Sense Multiple Access/Collision Detect
CSU	Channel Service Unit
CTS	Clear to Send
DAA	Designated Approving Authority
DAAR	Designated Approving Authority Representative
DDoS	Distributed Denial of Service
DECC-D	Defense Enterprise Computing Center - Detachment
DES	Data Encryption Standard
DFAS	Defense Finance and Accounting Service
DIAP	Defense-Wide Information Assurance Program
DiD	Defense-in-Depth
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DLA	Defense Logistics Agency
DMZ	Demilitarized Zone
DNACI	Department of Defense National Agency Check Plus Written Inquiries
DNS	Domain Name Service (server)
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoD R	Department of Defense Regulation
DoD STD	Department of Defense Standard
DoJ	Department of Justice
DoS	Denial of Service
DRP	Disaster Recover Plan
DSR	Data Set Ready
DSS	Defense Security Service
DSU	Data Service Unit

DTR	Data Terminal Ready
EC/EDI	Electronic Commerce/Electronic Data Interchange
EIA	Electronic Industry Association
EIA/TIA	Electronic Industry Association/Telecommunications Industry Association
ENTNAC	Entrance National Agency Check
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standards
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FTP	File Transfer Protocol
GIG	Global Information Grid
GOCO	Government Owned, Contractor Operated
HA	Health Affairs
HDBK	Handbook
HDT	Help Desk Technician
HIPAA	Health Insurance Portability and Accountability Act
HP	Hewlett Packard
HTTP	Hyper Text Transfer Protocol
I&A	Identification and Authentication
IA	Information Assurance
IATA	Information Assurance Technical Advisory
IATO	Interim Approval to Operate
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IAW	In accordance with
IAWG	Information Assurance Working Group
ICMP	Internal Control Message Protocol
ID	Identification
IDS	Intrusion Detection System
IKE	Internet Key Exchange
IM	Information Management

IM PRB	Information Management Program Review Board
IMT&R	Information Management, Technology and Reengineering
INFOSEC	Information Security
IOS	Internetwork Operation System
IP	Internet Protocol
IPSec	Internet Protocol Security
IR	Infrared
IrDA	Infrared Data Association
IS	Information System
ISP	Internet Service Provider
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
JID	Joint Intrusion Detector
JTF	Joint Task Force
KM	Knowledge Management
KMI	Key Management Infrastructure
LAN	Local Area Network
LCM	Life-Cycle Model
LEA	Law Enforcement Agency
LEC	Local Exchange Carrier
MAC	Media Access Control
MAC	Mission Assurance Category
MAIS	Major Automated Information System
MDAP	Major Defense Acquisition Program
MHS	Military Health System
MIL	Military
MNS	Mission Needs Statement
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Management Plan
MTF	Military Treatment Facility

MVS	Multiple Virtual Storage
NAC	National Agency Check
NACI	NAC Plus Written Inquiries
NCSC	National Computer Security Center (at NSA)
NET	Network
NIAP	National Information Assurance Partnership
NIC	Network Interface Card/Network Information Center
NIPRNet	Non-Secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NNTP	Network News Transfer Protocol
NSA	National Security Agency
NSO	Network Security Officer
NSOC	Network Security Operations Center
NT	Near Term
OASD	Office of Assistant Secretary of Defense
OMB	Office of Management and Budget
OPM	Office of Personnel Management
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
OUI	Organizationally Unique Identifiers
OUS&P	Outside the United States and Possessions
PAN	Personal Area Network
PC	Personal Computer
PC S	Personal Communications System
PDA	Personal Digital Assistant
PED	Personal Electronic Device
PEO	Program Executive Officer / Program Executive Office
PID	Patient Identifiable Data
PIN	Personal Identification Number
PKE	Public Key Enabled
PKI	Public Key Infrastructure
PM	Program Manager -or- Project Manager
PMO	Program Management Office

POC	Point of Contact
POP	Point of Presence / Post Office Protocol
PPP	Point-to-Point Protocol
PRB	Program Review Board
PUB	Publication
RA	Registration Authority
RADIUS	Remote Access Dial in User Server
RAM	Random Access Memory
RCERT	Regional Computer Emergency Response Team
RF	Radio Frequency
RFC	Request for Comments
RISC	Reduced Instruction Set Computer
RMON	Remote Monitoring
ROM	Read Only Memory
RS	Recommended Standard
RTS	Request to Send
SA	System Administrator
SBU	Sensitive But Unclassified
SCIF	Sensitive Compartmented Information Facility
SF	Standard Form
SFUG	Security Features User's Guide
SIPRNet	SECRET Internet Protocol Router Network
SKIP	Secure Key Interchange Protocol
SLIP	Serial Line Internet Protocol
S/MIME	Security Multipurpose Internet Mail Extension
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedures -or- Standing Operating Procedures
SPACECOM	Space Command
SPARC	Sun Scalable Processor Architecture
SPI	Security Profile Inspector
SSAA	System Security Authorization Agreement
SSH	Secure Shell
SSL	Secure Sockets Layer

ST&E	Security Testing and Evaluation
TA	Technical Advisory / Trusted Agent
TACACS	Terminal Access Controller Access Control System
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
Telnet	Telecommunications Network
TFTP	Trivial File Transfer Protocol
TG	Technical Guideline
TIA	Telecommunications Industry Association
TIWG	Technical Integration Working Group
TIMPO	Tri-Service Infrastructure Management Program Office
TLS	Transport Layer Security
TMA	TRICARE Management Activity
TMI&S	Technology Management, Integration and Standards
UDP	User Datagram Protocol
URL	Uniform Resource Locator
U.S.	United States
US&P	United States and Possessions
VCTS	Vulnerability Compliance Tracking System
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VTY	Virtual Terminal
WAN	Wide Area Network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WHS	Washington Headquarters Services
WLAN	Wireless Local Area Network
WWW	World Wide Web

Appendix D – Wireless Devices Policy

SUBJECT: Military Health System (MHS) Automated Information Systems (AISs) and Networks Wireless Devices Policy

References:
(a) DoD Draft Overarching Wireless Policy, V4.1, March 11, 2002
(b) DoDD 8500.1, "Information Assurance (IA)," October 24, 2002
(c) DoDI 5200.40, Defense Information Technology Security Certification and Accreditation Process (DITSCAP), 30 December 1997 (supplemented by DoD 8510.01-M, Applications Manual, July 2000)
(d) Federal Information Processing Standards Publication (FIPS Pub) 140-2, "Security Requirements for Cryptographic Modules," May 25, 2001

1. PURPOSE

This Policy:

1.1 Establishes a TRICARE Management Activity (TMA) and Tri-Service (centrally managed) policy for supporting Information Assurance (IA) in TMA and Tri-Service (centrally managed) Automated Information Systems (AISs) and networks when incorporating wireless services, devices, and technological implementations in accordance with (IAW) Reference (b) above.

1.2 Promotes interoperability through maximum use of standardization throughout TMA and Tri-Service (centrally managed) AISs and networks for wireless services, devices, and technological implementations. Promotes increased sharing by all DoD activities of wireless expertise through the knowledge management process.

1.3 1.3 Requires proactive management of the use of wireless services, devices, and technological implementations.

2. APPLICABILITY AND SCOPE

This Policy/Guidance:

2.1 Applies to all TMA and Program Executive Office (PEO) personnel, including contractors, and visitors using wireless devices who have access to either TMA or Tri-Service (centrally managed) AISs and networks under the authority of the Military Health System (MHS) Chief Information Officer (CIO). To maximize standardization of security across the MHS, Service Medical Department personnel are encouraged to use this document as IA guidance for the AISs and networks developed, managed, and operated by the Services.

2.2 Applies to all wireless devices and technologies, including voice and data capabilities, that can operate either as part of the networked Global Information Grid (GIG) [reference (b)], or as non-GIG Information Technology (IT) (stand-alone systems).

This includes, but is not limited to commercial wireless networks and all Portable Electronic Devices (PEDs), such as laptop computers, cellular/Personal Communications System (PCS) devices, audio/video recording devices, scanning devices, messaging devices, Personal Digital Assistants (PDAs), and any other device capable of storing, processing, or transmitting information.

2.3 Does not apply to hearing aids, pacemakers, other implanted medical devices, and personal life support systems.

3. DEFINITIONS

Enclosure 1 defines terms used in this issuance.

4. POLICY

The following minimum requirements apply when using wireless devices, services, and technologies.

4.1 Classified Information – MHS wireless devices shall not be permitted to store, process, and/or transmit classified information.

4.2 Sensitive But Unclassified (SBU) Information – Only wireless devices that are procured, configured, maintained, and are government owned shall interface with the TMA and Tri-Service (centrally managed) AISs and networks. The following minimum requirements are directed for each basic area of security in wireless processing.

4.2.1 Identification and Authentication (I&A) – Strong authentication and personal identification is required for access to the TMA and Tri-Service (centrally managed) AISs and networks IAW Defense Information Technology Security Certification and Accreditation Process (DITSCAP) [reference (c)]. I&A measures shall be implemented both at the device and network level.

4.2.2 Confidentiality – Encryption for transmission of sensitive but unclassified (SBU) information from and to wireless devices is required. Encryption must be implemented end-to-end over an assured channel and shall meet the FIPS 140-2 standard [reference (d)], at a minimum. The DAA is authorized to grant individual exceptions on a case-by-case basis to the requirement for encryption IAW reference (c).

4.2.3 Data Integrity – Wireless devices themselves store and process information but often do not have the same degree of standard protections afforded by standard desktop operating and file management systems. The Designated Approving Authority (DAA) shall give special consideration to implementations of wireless devices for processing data and shall ensure that the MHS requirements are followed by all government personnel and contractors storing and processing protected health information, IAW reference (b).

4.2.4 Availability – Wireless devices are inherently vulnerable to denial of service attacks. The DAA shall give special consideration to implementations of wireless devices to ensure measures are taken to mitigate these risks. These risks include not only threats from the outside, but potential interference from friendly sources, IAW reference (b).

4.3 Wireless devices shall not be connected to TMA and Tri-Service (centrally managed) AISs and networks without the approval of the appropriate DAA. If wireless devices are connected to TMA and Tri-Service (centrally managed) AISs and networks, the DAA shall specify implementation processes for risk mitigation strategies (e.g., virus protection, mobile code restrictions).

4.4 Use of wireless devices that interface with the TMA and Tri-Service (centrally managed) AISs and networks shall require a signed user agreement for each device (Enclosure 2). The DAA will ensure there are signed user agreements for all wireless devices operating under his/her cognizance.

4.5 The DAA shall require a risk assessment on AISs and networks upon introduction of wireless technologies, to include those creating an interface to non-TMA and Tri-Service (centrally managed) AISs and networks. The risk assessment shall specifically address the wireless risk mitigation, IAW DITSCAP.

4.6 The DAA shall consider the unintentional introduction of risk associated with wireless technologies as part of any DITSCAP.

4.7 The DAA shall ensure implementation of mitigating actions against wireless device vulnerabilities described in Enclosure 3.

4.8 Joint, Combined, and Coalition Interoperability – When TMA and Tri-Service (centrally managed) AISs and networks wireless technology is used to support joint, combined, and coalition operations, the infrastructures and devices shall be required to be interoperable, and support the widest range of joint functions, missions, and operational scenarios. Exceptions are authorized for activities evaluating new technologies.

4.9 Spectrum Management

4.9.1 Wireless device implementers shall coordinate the use of wireless devices, including commercial unlicensed devices.

4.10 Knowledge Management (KM). TMA and PEO staff shall consult the DoD wireless KM database to obtain DoD wireless information, to include information on vulnerability assessments, as well as best practices and procedures for wireless device configurations and connections. This database will be utilized by DAAs to help determine acceptable uses of wireless devices. The database will also be used to coordinate, prioritize, and avoid duplication of vulnerability assessments of wireless devices. (Uniform Resource Locator (URL) for the DoD wireless KM database is currently under development by Defense Information Systems Agency (DISA), it will be provided to MHS AISs and network users upon receipt.)

5. RESPONSIBILITIES

5.1 MHS CIO shall monitor and provide oversight for all TMA and PEO wireless activities.

5.2 DAAs or the designated representative shall:

5.2.1 Control wireless access to AISs and networks under their cognizance to minimize community risk. To ensure that the wireless systems (including external interfaces to commercial wireless services) do not introduce vulnerabilities that undermine the assurance of the other interconnected systems.

5.2.2 Coordinate and promulgate wireless policies and procedures. Monitor and provide oversight of wireless activities.

5.2.3 Establish a formal coordination process to ensure proper protection of information within the TMA and Tri-Service (centrally managed) AISs and networks employing wireless technologies.

5.2.4 Ensure interoperability of wireless capabilities in support of AIS and network operations.

5.2.5 Direct the development of acquisition strategies and assess potential architectures (e.g., wireless application frameworks) to minimize wireless systems/services cost, achieve economies of scale, and promote interoperability and security.

5.2.6 Direct TMA and PEO program managers to utilize the DoD wireless Knowledge Management Database to obtain shared information on wireless devices.

5.2.7 Ensure wireless requirements for information systems and functional applications developed under their cognizance are fully coordinated with the TMA Directors and/or Tri-Service Medical CIOs.

5.2.8 Deploy defensive actions necessary to deter or defeat unauthorized wireless activity, up to and including computer network attacks against TMA and Tri-Service (centrally managed) AISs and networks, and minimizes damage from such activities.

5.2.9 Ensure wireless interfaces to TMA or Tri-Service (centrally managed) AISs and networks are consistent with Federal and DoD policies.

5.2.10 Incorporate wireless topics into annual IA training. Provide initial security training specifying precautions for use of wireless devices, prior to issuance.

5.2.11 Ensure intrusion detection is integral to the wireless portion of AISs and Networks.

5.3 Responsibilities

5.3.1 Users shall report lost or stolen wireless devices to the DAA or appropriate designee within 24 hours of occurrence.

5.3.2 Users must sign a Wireless Device Usage Statement (Enclosure 2) following initial security training, signifying complete understanding of the procedures for wireless device operation in a TMA and Tri-Service (centrally managed) AISs and networks.

5.3.3 Users shall strictly adhere to agency policy on wireless devices.

6. <u>EFFECTIVE DATE</u>

This policy is effective immediately.

Enclosures – 3

1. Definitions
2. Wireless Device Usage Statement
3. Mitigating Actions Against Wireless System Vulnerabilities

Wireless Devices Policy – Enclosure 1

DEFINITIONS

Automated Information System (AIS). Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data and includes computer software, firmware, and hardware. Note: Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment.

Assured Channel. A network communication link that is protected by a security protocol providing authentication, confidentiality and data integrity, and employs DoD approved cryptographic technologies whenever cryptographic means are utilized. The following protocols and mechanisms are sufficient to meet the requirements of authentication, confidentiality and data integrity protection for an assured channel: The Secret Internet Protocol Router Network (SIPRNet); Internet Protocol Security (IPSec); Secure Sockets Layer (SSL); Transport Layer Security (TLS); Secure Multipurpose Internet Mail Extension (S/MIME); and other systems using NSA-approved high assurance guards with link encryption methodology.

Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. (NSTISSI No. 4009 rev 1, January 1999.)

Community Risk. A combination of (1) the likelihood that a threat will occur within an interacting population; (2) the likelihood that a threat occurrence will result in an adverse impact to some or all members of that populace; and (3) the severity of the resulting impact.

Designated Approving Authority (DAA). The official designated by the local authority, which has the power to decide on accepting the security safeguards prescribed for an information system.

Federal Information Processing Standards (FIPS). The National Institute for Standards and Technology (NIST) Federal Information Processing Standards validation program.

Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD approach for identifying information security requirements, providing security solutions, and managing information technology system security. (DoD Instruction 5200.40 [reference (c)].)

End-to-End. The term end-to-end is most often used in discussions regarding system testing and includes consideration of connectivity, data exchange capability, and the business-scenario-specific data being processed. Use of the term in other contexts should still include the three components.

External Interfaces. Interfaces that include commercial systems (such as a cellular/PCS or pager network not under control of the DAA) which may carry data between systems under control of the DAA (the TMA and Tri-Service (centrally managed) AISs and networks and a TMA and Tri-Service wireless device).

Global Information Grid (GIG).

(a) The globally interconnected, end-to-end set of information capabilities associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in Section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

(b) Includes any system, equipment, software, or service that meets one or more of the following criteria:

(1) Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

(2) Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from, or transmitted to, other equipment, software and services

(3) Processes data or information for use by other equipment, software and services

(c) Non GIG IT – Stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network.

Identification & Authentication (I&A). Process an information system (IS) uses to recognize an entity and establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Information Assurance (IA). Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation.

Information System (IS). The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

Mission Assurance Category (MAC). Applicable to MHS centrally managed information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

- **Mission Assurance Category I (MAC I).** Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

- **Mission Assurance Category II (MAC II).** Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.

- **Mission Assurance Category III (MAC III).** Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.

Personal Digital Assistant (PDA). A generic term for a class of small, easily carried electronic devices used to store and retrieve information.

Personal Area Network (PAN). A system that provides electromagnetic communication connectivity over a few yards. Currently it uses either radio or infrared technology.

Portable Electronic Device (PED). Any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting information, i.e., PDA, cellular/PCS telephones, two-way pagers, e-mail devices, audio/video recording devices, and hand-held, notebook, or laptop computers.

Public Key Infrastructure (PKI). A PKI is that portion of the security management infrastructure dedicated to the management of keys and certificates used by public key-based security services. A PKI is a credentials service; it associates user and entity identities with public keys. A well-run PKI is the foundation on which the trustworthiness of public key-based security mechanisms rests.

Synchronize or Hot-Synch. The process of communicating with a host or another wireless device to upload, download, merge, or swap information.

Wide Area Network (WAN). A system that provides regional, national, or global communication coverage.

Wireless Application Protocol (WAP). An open, global specification that allows mobile users with wireless devices to easily access and interact with information and services.

Wireless Device. Any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting information (i.e., PDA, cellular/PCS telephones two-way pagers, e-mail devices, audio/video recording devices, and hand-held, notebook, or laptop computers).

Wired Equivalent Privacy (WEP). An algorithm, which is part of the 802.11 standard, is used to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network; this function is not an explicit goal in the 802.11 standard, but it is frequently considered to be a feature of WEP.

Wireless. Technology that permits the transfer of information (active or passive) between separated points without physical connection. Currently wireless technologies use infrared (IR) and radio frequency (RF), and optical wireless (a.k.a. “Free Space Optics”) but, as technology evolves, wireless could include other methods of transmission. Active information transfer entails emanation of energy, whereas passive information transfer includes stand-alone storage devices that can record audio and video information.

Wireless Devices Policy – ENCLOSURE 2

WIRELESS DEVICE USAGE STATEMENT

Wireless Device Information

1. Manufacturer: ______________________ Model: _______________ Serial Number: _________________________
2. Software Installed on Wireless Device: ____
3. Department where Wireless Device will be located/used: ______________________________________
4. Property Account Number of CPU or designated server on which wireless device software will be installed: _______

Wireless Device Policy

1. Wireless Device:
   a. Will be secured when not in use.
   b. Will only be connected to the Information System listed above.
   c. Will conform to approved DoD standards of operation for Information Systems.
   d. May be used to carry information from a desktop workstation, including schedules, contact information, notes, and e-mail items from Microsoft Outlook.
   e. May be used to take notes, save information, or write e-mails while away from Wireless Device user's desk.
   f. May be used to synchronize information with Wireless Device user's desktop workstation using direct connect cables .
2. Wireless devices will <u>NOT</u> be:
   a. Used to process or store classified information.
   b. Connected to any classified Information System or network.
   c. Used with modems to exchange information with Wireless Device user's desktop or other systems on the network.
   d. Used to synchronize any equipment features or devices across any network.
   e. Used to download and install freeware or shareware software enhancements to wireless devices. Such software is from untrusted sources and may contain malicious code.
   f. Left unattended while attached to a government Information System.
3. Please contact your Information Systems Security Manager (ISSM) if you have any questions or concerns regarding this policy.

Wireless Device Use Agreement

1. I have read and understand the security guidelines in the Wireless Use Policy. I further understand the necessity for safeguarding my Wireless Device and recognize the requirement for maintaining confidentiality of all data stored in it.
2. I agree to abide by the strict policy outlined above and understand that failure to comply will result in the loss of my Wireless Device use privilege.

ISSM Information

Name: ____

Title: ____

Date: ____

Signature: ____________________________________

User Information

Name: ____

Title: ____

Date: ____

Signature: ____________________________________

DAA APPROVAL: ____ DATE: ____________________

Remember that your Wireless Device is FOR OFFICIAL USE ONLY.
Personally owned wireless devices are NOT authorized.

Wireless Devices Policy – ENCLOSURE 3

MITIGATING ACTIONS AGAINST WIRELESS SYSTEM VULNERABILITIES

E3.1 Personal Area Networks (PAN)

E3.1.1 PAN technologies (including Bluetooth) transmitting classified information is prohibited.

E3.1.2 PAN technologies shall not be utilized for transmitting SBU information unless the data is encrypted end-to-end with a FIPS 140-2 Overall Level 1 (Triple-DES or better) -approved encryption algorithm. Current BlackBerry devices may be utilized due to the use of FIPS 140-2-approved encryption algorithms, while Bluetooth technology is considered unacceptable as it has not been verified. With Bluetooth and 802.11, ad hoc networking may occur without the user's knowledge.

E3.2 Wireless Local Area Network (WLAN)

E3.2.1 Classified information over TMA and Tri-Service (centrally managed) AISs and networks WLANs is not permitted.

E3.2.2 For SBU information, WLANs shall use FIPS 140-2 Overall Level 1 (Triple-DES or better) encryption. The wired equivalent privacy (WEP) security protocol built into the current 802.11 standard for wireless LANs does not use a FIPS 140-2 approved encryption algorithm and has been found by the cryptographic community to have fundamental flaws.

E3.2.3 If third party hardware or software virtual private network (VPN) technology is used to meet the requirement of FIPS140-2 it shall also be IPSec (International Computer Security Association Labs or VPN Consortium) certified for interoperability.

E3.2.4 Wireless Access Points (APs) shall only be placed in an isolated sub-network or Virtual LAN (VLAN) located outside the local TMA and Tri-Service (centrally managed) AISs and networks' network security boundary.

E3.2.5 Wireless APs shall not be configured over a wireless link; only via a console connection.

E3.2.6 Hyper Text Transfer Protocol (HTTP) interfaces shall be turned off after initial configuration.

E3.3 Wireless devices – (Including PDAs, cellular/PCS phones, messaging devices, audio/video recording devices, scanners, and hand-held, notebook, or laptop computers)

E3.3.1 Wireless devices shall not be used to store, process, and/or transmit SBU information unless adequate security mechanisms are provided to protect the information from compromise as prescribed in 4.1 and 4.2. Wireless devices shall not be used to store, process, and/or transmit classified information.

E3.3.2 Wireless devices shall not be permitted inside classified areas.

E3.3.3 Wireless solutions could create backdoors into TMA and Tri-Service (centrally managed) AISs and networks. If a device receives information via a wireless technology and that device allows that information to be placed directly into TMA and Tri-Service (centrally managed) AISs and networks at the workstation level, then all perimeters and host-based security devices have been bypassed. Therefore, wireless devices that are connected directly to TMA and Tri-Service (centrally managed) AISs and networks (e.g., via a hot-synch connection to a workstation) shall not be permitted to operate. Note: an ad-hoc connection using IR, Bluetooth, or 802.11 peer could be used to pass malicious code into the device while it isn't in the cradle. The device could then be commanded to extract information from the TMA and Tri-Service (centrally managed) AISs and networks when it is placed in the cradle for later recovery.

E.3.3.4 The use of TMA and Tri-Service (centrally managed)-approved anti-virus software on wireless devices is mandatory. Where antivirus software is not yet available for a device, the synchronization capability should be disabled. To ensure consistent levels of protection required against viruses, it is required to maintain up-to-date signature files that are used to profile and identify viruses, worms, and malicious code as approved by the appropriate DAA. The network infrastructure shall accommodate virus software updates for all wireless devices and their supporting servers. DISA maintains a list of approved wireless anti-virus software.

E3.3.5 Wireless devices are easily lost or stolen. To protect against loss of sensitive information, the use of DoD-approved file system/data store encryption software on wireless devices is mandatory. Encryption software for applicable wireless devices will be available at a site maintained by DISA.

E3.3.6 Wireless devices with SBU information shall be capable of being erased, zeroized or overwritten to the satisfaction of the appropriate DAA. If used to store, process, and/or transmit SBU information deemed no longer needed, and cannot be erased/zeroized/overwritten to the satisfaction of the appropriate DAA, it shall be physically destroyed in a manner that ensures that stored data is not recoverable.

E3.3.7 Wireless devices that support the Wireless Application Protocol (WAP) and utilize commercial wireless network providers are at risk for information compromise. Data shall not be transmitted in this situation unless it can be assured that data is end-to-end using a FIPS 140-2-Level 1 approved encryption algorithm. The WAP standard is evolving to support data confidentiality requirements through the use of PKI digital certificates and by allowing customers to run their own WAP gateways for secure, direct connections to TMA and Tri-Service (centrally managed) AISs and network application platforms. All interfaces between the wireless network and the wired network should be treated as if they are wired interfaces to the outside world and all the methods used for protecting a wired interface should be placed between the wireless device and the wired network.

E3.4 Cellular/PCS and wireless e-mail devices.

E3.4.1 Cellular/PCS and wireless e-mail devices are subject to several vulnerabilities (e.g., interception, scanning, and remote command to transmit mode). Therefore, cellular/PCS and wireless e-mail devices that are used to transmit SBU information shall only be used when specifically approved by the appropriate DAA. The cellular/PCS and wireless e-mail devices shall not be allowed into a Sensitive Compartmented Information Facility (SCIF) or other classified area (per section 4.2) unless it is rendered completely inoperable. Turning off a Cellular/PCS & wireless e-mail device may not prevent remote activation on a device having a sleep mode.

E3.4.2 Information transmission devices with a connection to a commercial wireless infrastructure (e.g., cellular/PCS and pagers) are particularly vulnerable to probability of intercept/detection and/or traffic profiling because the radio link is exposed for several miles and may be subject intrusion attacks. Therefore, these devices and network management systems (e.g., geo-location and subscriber identification) must be protected.

E3.5 Spectrum

E3.5.1 Licensed devices – The DoD is required to obtain radio frequency guidance prior to contractual obligations for full-scale implementation. A DD Form 1494 is necessary to submit for spectrum certification. This process reviews the equipment's characteristics for supportability and conformance to the national frequency allocation tables in the NTIA manual. Wireless devices intended for use outside the United States and Possessions (OUS&P) require host nation approval. Each country has its unique frequency allocation tables, therefore, coordination and approval must be done with each country where use is intended (i.e., a military frequency allocated in the United States is not recognized as an allocated frequency for the same use in other countries). The DD Form 1494 is required for this approval. A frequency assignment is necessary once the spectrum certification is complete. This process gives the authority to transmit on a specific frequency within set parameters such as power level, antenna gain, and location.

E3.5.2 Non-licensed devices – Non-licensed devices must conform to the FCC, Part 15 rules and are exempt from the spectrum certification and frequency assignment process when used in the United Stated and Possessions (US&P). Any change or modification to a non-licensed Part 15 device, such as boosting the power, invalidates the conformance to Part 15, thus the user must apply for spectrum certification. Users of non-licensed devices that intend for use OUS&P must submit a DD Form 1494 for host nation coordination/approval. TMA and Tri-Service activities will not indiscriminately use non-licensed devices for critical tactical or strategic command and control applications essential for mission success, protection of human life, or protection of high-value assets. Non-licensed devices must accept interference from any other federal, non-federal, or civilian electronic system, therefore, offer no protection of spectrum use in support of operational requirements. If non-licensed devices cause interference to a licensed user, the non-licensed user must cease operation. It is recommended that licensed devices be considered as the primary equipment.

E3.6 Intrusion Detection and Electromagnetic Sensing

The wireless systems shall also be subject to active penetration and other forms of testing, such as electromagnetic sensing IAW TMA policy and restrictions. Active electromagnetic sensing at TMA or contractor premises to detect/prevent unauthorized access of TMA and Tri-Service (centrally managed) AISs and networks shall be periodically performed by the appropriate DAA and Defense Security Service (DSS) office to ensure compliance with the DITSCAP, [reference (c)] ongoing accreditation agreement. Electromagnetic sensing shall be used to detect unauthorized Wireless LANs, unauthorized or improperly secured Bluetooth transmitters, or other security breaching backdoors to TMA and Tri-Service (centrally managed) information systems.

Appendix E - Military Health System Information Assurance Vulnerability Alert (IAVA) Process

1. PURPOSE:

1.1. The Department of Defense (DoD) has designated the Defense Information Systems Agency (DISA) as the DoD Agent for the Information Assurance Vulnerability Alert (IAVA) process. DISA, acting as the DoD Computer Emergency Response Team (CERT) will disseminate vulnerability alerts to the CINC, Service, and Agency point of contacts and track the alerts to the POCs for compliance. The DoD Military Health System (MHS) IAVA policy creates the central IAVA coordination desk, as required by Office of the Secretary of Defense (OSD). This appendix prescribes procedures, and establishes responsibility for implementation and administration of the IAVA process for the release and dissemination of vulnerability advisories for Tri-Service and TMA AISs and networks to the appropriate Tri-Service and TMA Program Offices.

1.2. The IAVA process, which includes notification and mitigation, is intended to provide a means of obtaining positive control down to the system asset level. For the IAVA process to be successful, it must be incorporated into the configuration management processes. It is recommended that acquisition documents for MHS systems maintenance incorporate tasking language for testing information assurance vulnerability patches. This testing should ensure that patches resolve the potential vulnerability and simultaneously avoid negatively impacting the system's functionality, i.e., regression testing. This policy provides a single point of reference on how the MHS will implement and maintain a proactive IAVA process for Tri-Service and TMA AISs and networks.

1.3. The process relies on an automated management system, which employs two distinct tools: an IAVA notification system (commonly referred to as the IAVA system) and the Vulnerability Compliance Tracking System (VCTS). The IAVA notification system is used to issue vulnerability alerts, bulletins, and technical advisories. The VCTS is used to document compliance status at the asset level. The VCTS data is rolled up to the IAVA notification system for a compliance view across the DoD Component.

2. APPLICABILITY AND SCOPE:

2.1. THE GUIDANCE AND POLICY APPLIES TO:

2.1.1. All organizational Information Technology (IT) Program Offices within the TMA.

2.1.2. The detection and reporting of external DoD threats to the Tri-Service and TMA AISs and networks including, but not limited to, intrusion attempts, attempts to introduce malicious code, denial of service attempts, vulnerabilities in software used on any AIS or network, or any attempts intended to reduce the effectiveness of MHS operations that require acknowledgement and tracking of corrective action.

3. POLICY:

3.1. IT IS MHS POLICY THAT:

3.1.1. Tri-Service and TMA IT assets that are susceptible to vulnerabilities shall be registered in VCTS; specifically, this includes routers, firewalls, servers, and operating systems.

3.1.2. IAV Alert notifications and advisory patches will be reviewed, analyzed, and tested by Tri-Service and TMA System Program managers to determine impact, applicability, and methodology for implementation. Patches will be applied centrally if possible; or instructions will be provided to all system administrators for local implementation. Timely and accountable action is required to ensure the security and integrity of MHS information systems.

4. ROLES AND RESPONSIBILITIES:

4.1. DESIGNATED APPROVING AUTHORITY (DAA)

4.1.1. The DAA will make final IAVA related risk management and extension decisions for systems under his/her control.

4.1.2. DAAs are responsible for maintaining awareness of system vulnerabilities and the potential impact to their organization. They are ultimately accountable for ensuring an acceptable resolution is in place for vulnerabilities on each of their affected systems. IAVA compliance is an accreditation requirement for all systems and networks, and must be documented as part of each System Security Authorization Agreement (SSAA).

4.2. MHS IA OFFICE

4.2.1. The MHS IA Office will monitor their organization’s process for managing IAVA notifications and ensure that receipt is acknowledged, as appropriate. They will assist the DAAs in monitoring the activities of each Information Systems Security Manager (ISSM)/Information Systems Security Officer (ISSO)/System Administrator (SA) in response to IAVA notifications.

4.3. INFORMATION SYSTEMS SECURITY MANAGERS (ISSMS)/INFORMATION SYSTEMS SECURITY OFFICERS (ISSOS)

4.3.1. ISSMs/ISSOs are the organization’s action officers of record for the IAVA compliance process. Each ISSM/ISSO has the following responsibilities:

4.3.1.1. Provide status reports to the DAA.

4.3.1.2. Disseminate information about vulnerabilities and the potential impact within their organization.

4.3.1.3. Monitor the progress of their System Administrators (SAs) in eliminating vulnerabilities for their systems.

4.3.1.4. Work with their SAs to assess the impact of vulnerabilities across their organization and to ensure vulnerabilities are corrected.

4.3.1.5. Act as the organization's official point of contact for waiver requests.

4.3.1.6. Serves as alternate VCTS point of contact.

4.4. SYSTEM ADMINISTRATORS (SAS)

4.4.1. SAs are responsible for the management of IAVA notifications and implementation of corrective action at the asset level, as well as for registration and timely maintenance of assets under their control. They are responsible for acknowledging receipt of the IA vulnerability alert, bulletin, and technological advisory messages within five (5) working days; assessing the impact of the vulnerability on their system; and implementing the correction or requesting a waiver, as appropriate. SAs will provide an estimated completion date for the correction to be completed, and will coordinate the potential impact and estimated completion date with their ISSO. In addition, SAs must update the SA information and authority recorded in the VCTS whenever changes occur to SA assignment, systems, or system assets.

4.5. MHS IAVA DESK MONITOR

4.5.1. Upon initial notification by the DoD CERT IAVA notification, the MHS IAVA Desk Monitor will ensure the Tri-Service and TMA Program Offices receive the notification.

4.5.2. The Program Offices POCs will report back to the VCTS and the MHS IAVA Desk Monitor on the resolution of the alert.

4.5.3. The MHS IAVA Desk Monitor will ensure reporting requirements are met by read-only access to the VCTS.

4.6. TRI-SERVICE AND TMA PROGRAM OFFICES IAVA POC WILL:

4.6.1. Upon receipt of an IAVA , contact their ISSM/ISSO to ensure that the alert is acknowledged within 72 hours.

4.6.2. Ensure that the SAs check for damage to the network by exploitation of the vulnerability.

4.6.3. Ensure SAs resolve the vulnerability, report compliance back to the VCTS, and notify the MHS IAVA Desk Monitor as to the status of resolution to the IAVA notice.

4.6.3.1. Compliance information shall include at a minimum: number of assets affected, number of assets in compliance, and number of assets with extensions. For reporting purposes, assets include all components (i.e., servers, workstations, etc.) of Tri-Service and TMA information systems comprising or accessing a networked environment.

4.6.3.2. Maintain configuration control of information and documentation that identifies specific system/assets owners and system administrators(s), including applicable electronic addresses.

4.6.3.3. Establish a process to periodically review any extensions prior to their expiration date.

APPENDIX F – MHS PUBLIC KEY INFRASTRUCTURE (PKI)/PUBLIC KEY ENABLING (PKE) GUIDANCE

References:

(a) DoD Chief Information Officer Memorandum, subject: "Department of Defense Public Key Infrastructure," 12 August 2000

(b) DoD Chief Information Officer Memorandum, subject: "Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DoD)," 17 May 2001

(c) "X.509 Certificate Policy for the United States Department of Defense," Version 5.2, 13 November 2000

(d) "Public Key Infrastructure Implementation Plan for the Department of Defense," Version 3.1, 18 December 2000

(e) "Public Key Infrastructure Roadmap for the Department of Defense," Version 5.0, 18 December 2000

(f) DoD Chief Information Officer Memorandum, subject: "Common Access Card," 16 January 2001

(g) DEPSECDEF Memorandum, subject: "Smart Card Adoption and Implementation," 10 November 1999

(h) Assistant Secretary of Defense Memorandum, "Public Key Infrastructure (PKI) Policy Update," 21 May 2002

(i) Office of the Secretary of Defense memorandum, "Common Access Card – Changes," 18 April 2002

1.0 Introduction

Department of Defense (DoD) Public Key Infrastructure (PKI) provides the needed services and facilities for secure information access, communication, messaging, and electronic commerce. As an element in the Defense-in-Depth strategy, DoD PKI will provide a solid foundation for Information Assurance (IA) capabilities across DoD. The DoD PKI seeks to maximize the use of Commercial-off-the-Shelf (COTS) security products and to develop Government-unique products only when necessary. The public key enabling (PKE) of designated networks, Web servers, and client software applications will take advantage of the security services provided by the PKI.

2.0 Purpose

This appendix provides guidance on accomplishing DoD PKI/PKE objectives. It is important that we maintain an awareness of DoD PKI/PKE activities and take steps necessary to ensure that resources are available to meet the mandated milestones identified in references (a) through (i). Section 14 contains a list of definitions.

3.0 Applicability and Scope

This guidance applies to programs and activities within the MHS managed by the Service Medical Departments, MHS Program Executive Office (PEO), Program Managers (PMs) of TMA managed systems, Tri-Service Infrastructure Management Program Office (TIMPO), and Information Management, Technology & Reengineering Directorate (IMT&R) Director of Operations. PKI activities for Military Treatment Facilities (MTFs) and Theater is being managed by the designated component in each Military Department. The scope of this plan is to provide high-level guidance that (1) identifies DoD requirements with timelines, (2) assigns high-level roles and responsibilities, (3) describes the overarching DoD PKI architecture, and (4) establishes a schedule for revising these guidelines as DoD PKI/PKE evolves. Responsible components are encouraged to develop specific guidance based on the milestones identified in Section 5.

4.0 DoD PKI Overview

PKI refers to the framework and services necessary to generate, issue, and manage public key certificates. The DoD PKI will provide authentication, data integrity, confidentiality, and non-repudiation capabilities. DoD PKI features an incremental, evolutionary approach using open standards based on commercially available products and services. References (c) through (e) are the three major planning documents for DoD PKI evolution.

Current infrastructure (PKI) is based on a Class 3 (Medium) level of assurance that is intended for applications handling medium value information in a low to medium risk environment. The Class 3 level of assurance will migrate to the Class 4 level of assurance that is intended for applications handling medium to high value information in any environment. DoD has chosen the Common Access Card (CAC) as the target PKI platform for individual PKI certificates. See references (f), (g), and (i). User certificates for Class 3 and target Class 4 PKI certificates will be issued on CACs. Until the CAC is fully implemented, user Class 3 certificates may be issued on software tokens. While the DoD PKI continues to evolve, existing PKI capabilities will remain operational to facilitate an efficient transition.

References (c) through (i) provide the details of the DoD PKI implementation and architecture. The DoD PKI architecture supports the three major elements of a PK enabled system: subscribers, registration, and certificate management. DoD PKI architecture has centralized Root Certificate Authority with a single level of Certificate Authorities (CA) and numerous decentralized registration components. Reference (e) establishes the details of the DoD architecture.

5.0 DoD PKI Mandated Requirements and Milestones

Reference (a) directs the development and execution of the DoD PKI and provides specific guidance for applying PKI services throughout the Department. Reference (h) updates guidance in references (a) and (b), and outlines plans for reissuing DoD PKI and PKE policy. A summary of PKI requirements and milestones is provided in Table 1.

Table 1. PKI Mandated Requirements and Milestones

PKI Mandated Requirements	Milestones
1. Unclassified, private Web servers shall be issued Class 3 DoD PKI server certificates	NLT December 2000
2. Registration capability for Class 3 PKI shall be implemented.	NLT December 2001
3. All DoD Users shall be issued Class 3 certificate on software or hardware (CAC) tokens.	NLT October 2003
4. Upgrade registration capability for the Target Class 4 PKI.	NLT October 2003
5. DoD organizations shall begin issuing Target Class 4 certificates.	NLT October 2003
6. All private DoD and DoD-interest Web servers located on unclassified networks shall require client identification and authentication using Class 3 user certificates.	NLT October 2003
7. All electronic mail (as distinct from organizational messaging) sent within the Department will be digitally signed.	NLT October 2003
8. DoD unclassified networks that authenticate users shall be enabled for hardware token (CAC), certificate-based (Class 3) access control. (See reference (b) for conditions.)	NLT October 2003
9. Class 3 certificates may be distributed on software tokens, as necessary.	Until October 2003
10. Mission Category I systems operating on unclassified networks shall migrate to Target Class 4 certificates and tokens.	NLT December 2003
11. DoD unclassified networks shall be enabled for hardware token (CAC), certificate-based (Target Class 4) access control.	NLT December 2003
12. Transition from Class 3 certificate to Target Class 4 certificate is required for client identification and authentication.	NLT December 2003
13. Class 3 certificates may be issued on hardware tokens (CAC).	Until December 2004

Reference (b) provides specific guidance for PK-enabling of networks, Web servers, and client software applications to provide security services at appropriate levels. A summary of PKE requirements and milestones is provided in Table 2.

Table 2. PKE Mandated Requirements and Milestones

PKE Mandated Requirements	Milestones
1. E-mail in all operating environments and Web applications in unclassified environments shall be PK enabled. E-mail applications to include Web e-mail applications shall support both digital signature and encryption services. All other Web applications shall support client authentication to the applicable private Web server at a minimum.	NLT October 2003
2. E-mail and Web applications shall be PK enabled to interoperate with Class 4 PKI for Mission Category 1 applications operating on unclassified networks.	NLT December 2003
3. Legacy Mission Category 1 applications operating on unclassified networks and that use or require the use of public key cryptography shall be PK-enabled to interoperate with Class 4 PKI. Legacy applications scheduled for phase-out or replacement by this suspense date may be exempted.	NLT December 2003
4. E-mail and Web applications shall be PK enabled to interoperate with Class 4 PKI for all other operating environments (other than Mission Category 1 applications).	NLT September 2007
5. All other legacy applications that use or require the use of public key cryptography shall be PK enabled.	NLT September 2007

6.0 Responsibilities and Office of Primary Responsibility (OPR)

Successful compliance with DoD PKI across MHS will involve the coordination of activities among the Military Departments, Service Medical Departments, MHS PEO, PMs of TMA managed systems, TIMPO, IMT&R Director of Operations, and Technology Management, Integration and Standards (TMI&S). In accordance with references (a), (b), and (h), Table 3 specifies the high-level PKI and PKE roles and responsibilities for the MHS.

Table 3. MHS Responsibility and Office of Primary Responsibility (OPR)

Responsibility	OPR
1. MTF PKI/PKE implementation.	Service Medical Departments (in accordance with Military Department guidance)
2. Develop and maintain registration process for individual subscribers to supplement Defense Enrollment Eligibility Reporting System/Real-time Automated Personnel Identification System (DEERS/RAPIDS) capabilities.	Service Medical Departments (in accordance with Military Department guidance) [MTF, service headquarters personnel] IMT&R Director of Operations [HA/TMA network users]
3. Identify networks, Web servers, and applications that are covered by references (a) and (b).	Service Medical Departments (in accordance with Military Department guidance) MHS PEO [centrally managed programs] PMs of TMA managed systems IMT&R Director of Operations [HA/TMA]
4. Issue, revoke, maintain records, and report status of server certificates.	Service Medical Departments (in accordance with Military Department guidance) MHS PEO [centrally managed programs] PMs of TMA managed systems IMT&R Director of Operations [HA/TMA]
5. PKI implementation, training and maintenance at Headquarters HA/TMA Network. PKE implementation for the Headquarters HA/TMA Network.	IMT&R Director of Operations
6. Oversee PK enabling of MHS centrally managed programs, to include identification, enabling, and testing.	MHS PEO [centrally managed programs] PMs of TMA managed systems
7. Oversee PK enabling of Service Medical specific programs, to include identification, enabling, and testing.	Service Medical Chief Information Officers (CIOs)
8. Coordinate the assessment of bandwidth impact of digital signature and encryption on the infrastructure.	Service Medical Departments (in accordance with Military Department guidance) IMT&R Director of Operations [HA/TMA] TIMPO
9. Maintenance of MHS PKI/PKE Guidance.	IMT&R/TMI&S

7.0 PKI Registration

Registration is the process that subscribers use to identify themselves to the PKI and to request certificates. Subscribers include individuals, their PK-enabled applications, servers, and network devices that use public keys. References (c) and (e) establish the DoD registration requirements and responsibilities.

Registration is accomplished by the interaction of subscribers and individuals acting in trusted roles. Section 7.3 describes the various registration components: Registration Authorities (RA), Local Registration Authorities (LRAs), Trusted Agents (TAs), and RAPIDS Verifying Officials (VOs). Sections 7.1 and 7.2 focus on subscribers and Section 7.3 provides an overview of the trusted roles. The registration process may differ for Theater and other situations as determined by DoD and the Military Departments.

7.1.0 Individual Subscribers

To attain the desired security assurance level, users will be issued identity, e-mail signature, and e-mail encryption cryptographic certificates. DoD PKI certificates will be issued to all active duty military personnel, members of the Selected Reserve, DoD civilian employees who have access to DoD Automated Information Systems (AIS) and networks, and eligible contractor personnel. Eligible contractor personnel must meet one of the following criteria:

1) Work inside the DoD (e.g. either on a MTF, clinic, or DoD office)
2) Work in an area that has been assigned a .mil domain name
3) Use Government Furnished Equipment (GFE)

Contractor personnel not within one of the eligible categories may purchase certificates from an approved External Certificate Authority. (See Section 9, External Certificate Authority.)

DoD PKI user certificates will be issued on CACs (hardware token) and general issuance will be conducted by VO/LRAs at Defense Enrollment Eligibility Reporting System/Real-time Automated Personnel Identification System (DEERS/RAPIDS) registration locations. The CAC will be the primary token platform for both Class 3 and Target Class 4 PKI certificates. Until the CAC is fully deployed, Class 3 certificates may be issued on software tokens (diskette). The CAC registration capability may be supplemented, on an as needed basis, as follows: (1) the IMT&R Director of Operations will manage any registration process for users of the Headquarters HA/TMA Network and (2) the Service Medical Departments, in collaboration with the Military Departments, will ensure that the registration capability for individuals assigned to MTFs, intermediate commands, and headquarters is available.

7.2.0 Servers

References (a) and (b) establish requirements for Server certificates (Secure Sockets Layer (SSL)) to be issued to designated servers. The MHS PEO, PMs of TMA managed systems, IMT&R Director of Operations, and Service Medical CIOs will ensure that servers under their ownership are identified and that the required DoD PKI server certificates are issued and records are maintained. Designated LRAs will authorize and manage the issuing, key recovery, and revoking of DoD PKI server certificates within MHS.

7.3.0 Trusted Roles

The trusted roles of RAs, LRAs, and TAs are determined by DoD PKI guidelines.

7.3.1 Registration Authorities (RAs)

RAs are responsible for verifying the subscriber's identity and the information that is entered into PK certificates and for requesting the certificate management services. DoD certificate management services are detailed in Section 2.4.3 of reference (e). Currently, MTF RAs are assigned by the respective Services. The RA for Headquarters HA/TMA resides at Washington Headquarters Service's (WHS) Communications and Directives office. RAs may designate LRAs to assist with the registration process for local subscribers. MTF RAs will follow the established guidelines of the Military Departments.

7.3.2 Local Registration Authorities (LRAs)

For the Service Medical Departments, the LRA designation will be made in coordination with the Military Departments. LRAs who issue individual PKI certificates for the users of the Headquarters HA/TMA Network will be designated by the IMT&R Director of Operations. LRAs who issue server certificates for servers owned by centrally managed programs will be designated by either the MHS PEO, PMs of TMA managed systems, or IMT&R Director of Operations.

LRAs will be trained through attendance at a National Security Agency (NSA) approved LRA course. The designated LRAs may act as the contingent registrars for the issuance of DoD PKI certificates (in accordance with the component's LRA Certificate Practice Statement (CPS)). In addition, LRAs may designate in writing, Trusted Agents to assist with the registration process.

The designated LRA(s) has the responsibility to verify users identity credentials and the physical existence of all hardware, such as Web servers, that receive DoD PKI certificates. LRAs will only issue individual user certificates on software tokens (diskette). The responsibilities of Military Department LRAs may be modified per specific DoD or Military Department Guidance.

7.3.3. Trusted Agents (TAs)

Where convenient, Trusted Agents can be used to reduce demands on the LRA. TAs are nominated at the request of an LRA by either the LRA or a person in authority. The role of TA requires no formal training.

7.3.4. DEERS/RAPIDS Verifying Officials (VOs)/LRAs

DEERS/RAPIDS VOs are specialized versions of LRAs and will register DoD subscribers who have already been enrolled into the DEERS system into the PKI and issue CACs containing PKI certificates.

8.0 Enabling of Networks and Applications

References (a) and (b) specify DoD policy and guidance for the PKE of networks, Web servers, and client software applications. Section 5 of this document provides a summary of the requirements and milestones. The Service Medical CIOs, MHS PEO, PMs of TMA managed systems, and the IMT&R Director of Operations are responsible for determining which networks, Web servers and applications are covered by references (a) and (b). (See Section 6.) PKI/PKE (of networks) activities for the MTFs and Theater is being managed by the designated component in each Military Department. All are encouraged to pay particular attention to the definitions of Web Applications, Private Web Server, Mission Category, and legacy application included in reference (b).

9.0 External Certificate Authorities

Contractors not eligible for DoD provided PKI certificates may purchase a PKI certificate that meets DoD requirements from External Certificate Authorities (ECAs). ECAs will operate under a process that delivers a level of assurance required to meet DoD business and legal requirements. An Interim ECA (IECA) capability is currently available. Information on ECA certificates may be obtained at http://www.disa.mil/infosec/pkieca. The General Services Administration (GSA) Access Certificates for Electronic Services (ACES) program may extend their program to support DoD requirements in the near future. Current ACES information can be obtained at http://hydra.gsa.gov/aces/.

10.0 Certification and Accreditation

The Certification and Accreditation (C&A) for the LRA workstations will be performed in accordance with the DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The System Security Authorization Agreement (SSAA) will document the results.

11.0 Revision Schedule

This document will be reviewed semi-annually, and or on an as needed basis, to ensure that this guidance remains consistent with evolving public key technology and DoD PKI/PKE policy and directives.

12.0 Effective Date

This guidance is effective immediately.

13.0 Point of Contact (POC)

The Point of Contact for this action is the Technology Management, Integration & Standards PKI Technical Manager. The manager may be reached at (703) 681-6779 or by electronic mail at TMISWeb@tma.osd.mil.

14.0 Definitions

Automated Information System (AIS): A combination of computer hardware and software, data, or telecommunications that performs functions such as collecting, processing, transmitting, and displaying information. This also encompasses an AIS environment that includes systems, applications, telecommunications, and other components of information technology.

Assurance Levels: The level of assurance of a public key certificate is the degree of confidence in the binding of the identity to the public keys and privileges. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates issued by a certificate management system. (See reference the DoD X.509 Certificate Policy reference (c) for detailed definitions and guidance on usage.)

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Certificate/PKI Certificate: A computer-generated record that ties the user's identification with the user's public key in a trusted bond. The certificate contains the following (at a minimum): a version number, a serial number, identity of the issuing Certification Authority and the user, the user's public key, and validity dates.

Certification Authority (CA): An entity authorized to create, sign, and issue public key certificates. A CA is responsible for all aspects of the issuance and management of a certificate (e.g. control over the enrollment process, the identification and authentication process, the certificate manufacturing process, publication of certificates, revocation of certificates, and re-key).

Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in managing and issuing certificates in relation to a specific Certificate Policy.

Class 3: (Formerly Medium) This level is intended for applications handling medium value information in a low to medium risk environment. This assurance level is appropriate for applications that require identification of an entity as a legal person, rather than merely a member of an organization. This assurance level requires that the end user register in person. This assurance level is subdivided into components distinguished by protection of the private key either in software or hardware tokens. See reference (a) for details.

Class 4: (Formerly High) This level is intended for applications handling medium to high value information in any environment. These applications require identification of an entity as a legal person, rather than merely a member of an organization. This level requires a hardware token for private key material.

Common Access Card (CAC): The CAC is a standard identification card, the principal card used to enable physical access to buildings, installations, and controlled spaces, and will be used to enable Information Technology systems and applications that access the Department's computer networks.

Confidentiality: Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Digital Signature: A transformation of a message using an asymmetric cryptographic system and a hash function such that a person having the initial message and the signer's public key can accurately determine if the transformation was created using the corresponding signer's private key. In addition, it can be determined if the initial message was altered after the transformation was made.

Directory: The directory is a repository or database of certificates, CRLs, and other information available online to users.

External Certificate Authority (ECA): An agent that is trusted and authorized to create, sign, and issue certificates to approved vendors and contractors for the purpose of enabling secure interoperability with DoD entities.

Encryption: The process of transforming data to an unintelligible form in such a way that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process.

Interim External Certificate Authority (IECA): A temporary/interim agent that is trusted and authorized to create, sign, and issue certificates to approved vendors and contractors for the purpose of enabling secure interoperability with DoD entities.

Integrity (Data Integrity): Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Key Recovery: The mechanisms and processes that allow authorized parties to retrieve the cryptographic key used for data confidentiality when the original key is lost or is otherwise unavailable.

Legacy Application: For the purpose of reference (b), a legacy application is either an existing application or one in development/procurement whose contract solicitation (request for proposal or equivalent) is released no later than 120 days after the date of reference (b).

Local Registration Authority (LRA): An individual assigned the responsibility of managing end user access to the PKI system. LRAs register users in the PKI system and provide assistance and information on PKI-related topics to users.

Mission Category I: Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. Information in these systems must be absolutely accurate and available on demand (may be classified information, as well as sensitive and unclassified information). See reference (b).

Network: A network is composed of a communications medium and all components attached to that medium, including two or more computers, whose responsibility is the electronic exchange of information using a cohesive set of protocols.

Non-Repudiation: Strong and substantial evidence of the identity of the signer, time, and context of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message, and the integrity of its contents.

Private Key: The part of a key pair to be safeguarded by the owner. A private key can be either a signature or key exchange key. Private signature keys are used to sign. Private key exchange keys are used with another party's public key to establish a shared key. It is computationally infeasible to determine a private key given the associated public key.

Private Web Server: A Web server that is designed for and/or provides information resources that are limited to a particular audience (i.e., DoD) or a subset thereof. This would include Web servers that provide interfaces to e-mail systems. Any DoD operated Web server that provides any information resources that are not intended for the general public shall be considered a private Web server and is subject to this policy. A private Web server restricts or attempts to restrict general public access to it. The common means of restriction are by the use of domain restriction (e.g., .mil and/or .gov), filtering of specific Internet Protocol (IP) addresses, User ID and/or password authentication, encryption (i.e., DoD certificates), and physical isolation.

Public Key: The part of a key pair released to the public. A private key can be either a signature or key exchange key. The signer's public signature key is used to verify a digital signature.

Public Key Certificate: (See Certificate)

Public Key-Enabled (PKE) Applications/Web Server/Network: A Public Key-Enabled (PK-Enabled) Application or Web server or network is one that can accept and process a DoD PKI X.509 digital certificate to support one or more application, server, or network-specific functions (digital signature, data encryption support, system/network access) that provide security services. PK-enabled applications interoperate with the DoD PKI to access public key certificates, revocation information (e.g. Certificate Revocation List (CRL)), and general information in public directories or repositories.

Public Key Infrastructure (PKI): The framework and services that provide the generation, production, distribution, control, tracking, and destruction of public key certificates.

Registration Authority (RA): The person assigned the responsibility of authorizing and managing the LRA's access to the PKI system. RAs are also responsible for revoking certificates when required.

Root Certification Authority: The Root CA is a trusted entity responsible for establishing and managing a PKI domain by issuing CA certificates to entities authorized and trusted to perform CA functions.

Subscriber: An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. Subscribers are the consumers of the products and services provided by a PKI and are individuals as well as software applications and hardware devices (such as firewalls and routers).

Token: A physical device (e.g. floppy diskette, CAC, smart card, PC Card, etc.) which is used to protect and transport the private keys of a user.

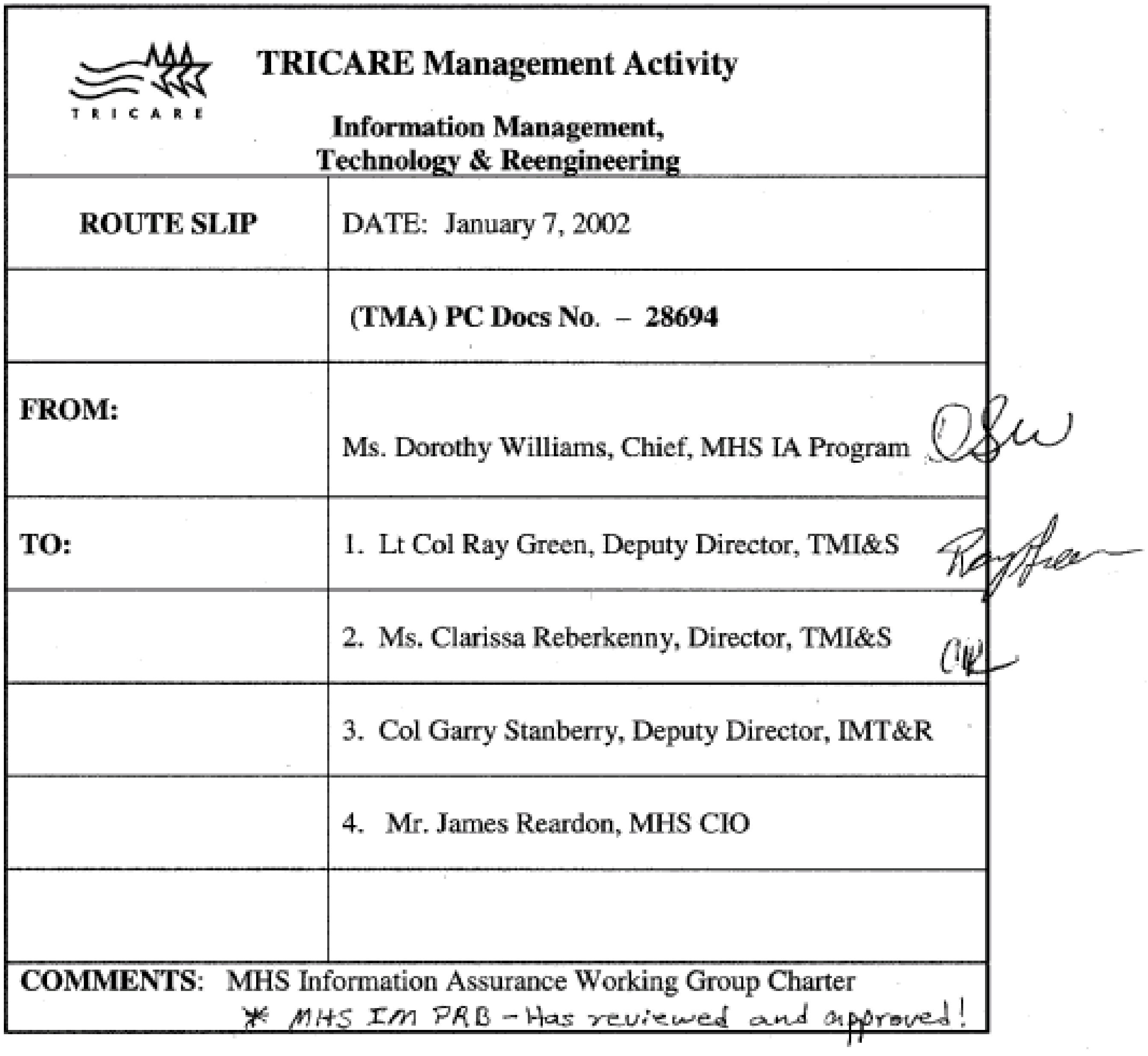
Trusted Agent (TA): An individual who supports an LRA by performing the face-to-face user authentication and dispenses the Certificate Registration Instruction (CRI) forms for the LRA. The TA role is optional, and can be used where needed to reduce the demands on a LRA.

User: A user is an individual or an organizational component represented by an individual that accesses the PKI system to acquire public/private keys and certificates. These keys are used to encrypt documents and other messages transmitted between computer systems.

Verification Officer (VO)/LRA: A DEERS/RAPIDS individual assigned the responsibility of issuing CACs and registering users in the PKI system.

Web-Application: Web browser and other distributed applications characterized by a Web interface and both back-end (server) and front-end (client) software.

Appendix G – MHS Information Assurance Working Group (IAWG) Charter



TRICARE

TRICARE Management Activity

Information Management,
Technology & Reengineering

ROUTE SLIP	DATE: January 7, 2002
	(TMA) PC Docs No. – 28694
FROM:	Ms. Dorothy Williams, Chief, MHS IA Program
TO:	1. Lt Col Ray Green, Deputy Director, TMI&S Ray Green
	2. Ms. Clarissa Reberkenny, Director, TMI&S CR
	3. Col Garry Stanberry, Deputy Director, IMT&R
	4. Mr. James Reardon, MHS CIO

COMMENTS: MHS Information Assurance Working Group Charter
* MHS IM PRB – Has reviewed and approved!

CHARTER

JAN - 8 2002

MILITARY HEALTH SYSTEM INFORMATION ASSURANCE WORKING GROUP

A. Purpose and Scope

The Military Health System (MHS) Information Assurance Working Group (IAWG) is hereby established to serve as a standing subcommittee of the MHS Information Management (IM) Program Review Board (PRB). The IAWG is a working-level body tasked to ensure that the MHS maintains a high level of Information Assurance (IA) for centrally managed Automated Information Systems (AISs) Networks.

B. Workgroup Functions

1. Evaluate, review, and make recommendations on IA issues for all MHS activities and organizations to the Technical Integration Working Group (TIWG) and the IM PRB.
2. Facilitate the exchange and sharing of IA information among the Army, Navy, Air Force, Department of Veterans Affairs, MHS Program Office Managers, and external partners.
3. Review Services, DoD and Federal IA policies and guidance and other security-related issues, and determine impact to the MHS.
4. Develop implementation criteria for MHS Program Offices to address new IA policies, procedures and technologies mandated by DoD.
5. Monitor the IA status of MHS programs and policies for compliance with Federal and DoD security regulations.

C. Membership

1. Chairperson, Chief, MHS IA Program
2. Principal IAWG Members
   a. Army Medical Department Representative

   b. Navy Medical Department Representative

   c. Air Force Medical Department Representative

d. Program Executive Office Security Representative

e. Technical Integration Working Group Representative

3. Associate IAWG Members

a. Clinical Information Technology Program Manager Representative

b. DoD Global Emerging Infections System Program Office Representative

c. Defense Medical Logistics Program Manager Representative

d. Executive Information/Decision Support Program Office Representative

e. Resources Information Technology Program Manager Representative

f. Theater Medical Information Program Manager Representative

g. Tri-Service Infrastructure Management Program Office Representative

h. TRICARE Management Activity, Aurora Representative

i. TRICARE Management Activity Directors

4. Ex Officio Members

a. Defense Information Systems Agency Representative

b. Joint Chiefs of Staff Representative – J4 Logistics Directorate

c. Veterans Health Administration Representative

d. Defense Healthcare Information Assurance Program Representative (Ft. Detrick)

D. Voting Privileges

Voting privileges are extended to the following members: Army, Navy and Air Force Medical Department Representatives, Program Executive Office Security Representative, and the Technical Integration Work Group Representative. In the event of a tie vote, the IAWG Chair will exercise a vote for tie breaking. All IAWG Members and alternates must be designated in writing by their Service or IA Program Managers to the IAWG Chair.

E. Chair Responsibilities

1. Call and chair the IAWG meeting.

2. Seek and represent IAWG consensus to the MHS IM PRB regarding IA issues discussed at meetings.

3. Establish subcommittees and working groups, as required, to address specific IA taskings or to develop specific IA solutions in support of IAWG initiatives.

4. Develop IAWG meeting schedules and agendas.

5. Ensure minutes are recorded and provided to the voting members within thirty days of each meeting.

F. Principal IAWG Member Responsibilities

1. Designate a primary and an alternate representative. Representation by the alternate is required in the absence of the primary member.

2. Participate in assessments of IAWG issues working towards a common enterprise-wide solution.

3. Implement and support IAWG decisions.

4. Provide representation for special assignments, working groups, and subcommittees, as required.

5. Advise the Chairperson of known or potential IA issues and/or problems associated with the MHS.

6. Review all read-ahead and presentation materials prior to the scheduled IAWG meeting and be prepared to discuss any issues. Principal members should also be prepared to vote on issues.

G. Operation

While any member of the IAWG can propose a topic for discussion, the voting members of the IAWG have the authority to determine what course of action, if any, will be taken. Meetings will be scheduled every month. Meetings are scheduled for a two-hour period. Special meetings may be convened at the call of the IAWG Chairperson to discuss issues of immediate importance. In the event that a voting member is unable to attend, the approved alternate member will attend and may exercise voting privileges. Members who cannot attend meetings will be afforded teleconference services whenever possible. Read-Ahead and briefing materials must be provided to the IAWG Chairperson no later than 12 noon EST, two days prior to the next scheduled IAWG meeting to ensure timely distribution. Non-compliance may lead to the cancellation or rescheduling of a briefing. This is necessary to allow other voting members the time and opportunity to review and prepare for discussion/vote on MHS issues.

H. Deliverables

The MHS IAWG will deliver IA reports and information papers resulting from its studies and analyses. The MHS IAWG will make recommendations to the IM PRB, the TIWG and the MHS CIO regarding IA issues. The recorder will prepare the IAWG meeting minutes, and following approval, will distribute the minutes to the members.

I. Charter Expiration

This charter will be reviewed annually by the MHS CIO with recommendations made by the IAWG members.

James C. Reardon
Chief Information Officer